2016-12

Analysis and augmentation of timing advance-based geolocation in LTE Cellular Networks

Roth, John D.

Monterey, California: Naval Postgraduate School

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

DISSERTATION

ANALYSIS AND AUGMENTATION OF TIMING ADVANCE-BASED GEOLOCATION IN LTE CELLULAR NETWORKS

by

John D. Roth

December 2016

Dissertation Co-Supervisors: Murali Tummala
John C. McEachen

Approved for public release. Distribution is unlimited.

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704–0188

1. AGENCY USE ONLY *(Leave Blank)*	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	December 2016	Dissertation

4. TITLE AND SUBTITLE

ANALYSIS AND AUGMENTATION OF TIMING ADVANCE-BASED GEOLOCATION IN LTE CELLULAR NETWORKS

5. FUNDING NUMBERS

6. AUTHOR(S)

John D. Roth

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Naval Postgraduate School
Monterey, CA 93943

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

N/A

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

The views expressed in this document are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol Number: N/A.

12a. DISTRIBUTION / AVAILABILITY STATEMENT

Approved for public release. Distribution is unlimited.

12b. DISTRIBUTION CODE

13. ABSTRACT *(maximum 200 words)*

The ubiquity of cellular technology has woven a variety of services, now axiomatic, into modern social fabric. Among those services is the ability to provide mobile user location. Applications of these location-based services include providing directions, emergency services, fraud protection, and direct marketing. This work provides in-depth analysis of cellular positioning, which leverages the Long Term Evolution (LTE) signaling plane timing advance (TA) parameter for the end of user geolocation. Additionally, we propose a novel method of augmenting TA-based positioning, Cellular Synchronization Assisted Refinement (CeSAR). We simultaneously show CeSAR to be a network performance multiplier and security vulnerability vis-a-vis the method's electromagnetically passive nature. Furthermore, we demonstrate how CeSAR improves positioning by adding system information and mitigating the effects of poor network infrastructure geometry. Through robust statistical analysis, we derive a theoretical lower bound on TA-based positioning and demonstrate that a statistically efficient estimator is possible in this context. Furthermore, numerical studies are conducted with synthetic and empirical data. The real-world data are observed in actual network deployments found in geographically diverse environments, such as Maryland and California. The results not only demonstrate the efficiency of the estimator but show that accuracy on the order of tens of meters is possible. Indeed, TA-based positioning is shown to be accurate on the order of 40 m in some scenarios. Additionally, we demonstrate that CeSAR is able to passively provide improvements ranging from 10 to 254 m over TA-only positioning.

14. SUBJECT TERMS

geolocation, Long Term Evolution (LTE), cellular networks, privacy, Cramer-Rao Lower Bound, quantization, maximum-likelihood estimation, timing advance

15. NUMBER OF PAGES 173

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UU

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2–89)
Prescribed by ANSI Std. 239–18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

ANALYSIS AND AUGMENTATION OF TIMING ADVANCE-BASED GEOLOCATION IN LTE CELLULAR NETWORKS

John D. Roth
Major, United States Marine Corps
B.S., United States Naval Academy, 2004
M.S., Naval Postgraduate School, 2012

Submitted in partial fulfillment of the
requirements for the degree of

DOCTOR OF PHILOSOPHY IN ELECTRICAL ENGINEERING
from the
NAVAL POSTGRADUATE SCHOOL
December 2016

Approved by:

Murali Tummala
Professor of Electrical and Computer Engineering
Dissertation Co-Supervisor and Committee Chair

John C. McEachen
Professor of Electrical and Computer Engineering
Dissertation Co-Supervisor

Gamani Karunasiri
Distinguished Professor of Applied Physics

Frank E. Kragh
Associate Professor of Electrical and Computer Engineering

James W. Scrofani
Associate Professor of Electrical and Computer Engineering

Approved by: R. Clark Robertson
Chair, Department of Electrical and Computer Engineering

Approved by: Douglas Moses
Vice Provost for Academic Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The ubiquity of cellular technology has woven a variety of services, now axiomatic, into modern social fabric. Among those services is the ability to provide mobile user location. Applications of these location-based services include providing directions, emergency services, fraud protection, and direct marketing. This work provides in-depth analysis of cellular positioning, which leverages the Long Term Evolution (LTE) signaling plane timing advance (TA) parameter for the end of user geolocation. Additionally, we propose a novel method of augmenting TA-based positioning, Cellular Synchronization Assisted Refinement (CeSAR). We simultaneously show CeSAR to be a network performance multiplier and security vulnerability vis-à-vis the method's electromagnetically passive nature. Furthermore, we demonstrate how CeSAR improves positioning by adding system information and mitigating the effects of poor network infrastructure geometry. Through robust statistical analysis, we derive a theoretical lower bound on TA-based positioning and demonstrate that a statistically efficient estimator is possible in this context. Furthermore, numerical studies are conducted with synthetic and empirical data. The real-world data are observed in actual network deployments found in geographically diverse environments, such as Maryland and California. The results not only demonstrate the efficiency of the estimator but show that accuracy on the order of tens of meters is possible. Indeed, TA-based positioning is shown to be accurate on the order of 40 m in some scenarios. Additionally, we demonstrate that CeSAR is able to passively provide improvements ranging from 10 to 254 m over TA-only positioning.

THIS PAGE INTENTIONALLY LEFT BLANK

Table of Contents

THIS PAGE INTENTIONALLY LEFT BLANK

List of Figures

THIS PAGE INTENTIONALLY LEFT BLANK

List of Tables

THIS PAGE INTENTIONALLY LEFT BLANK

List of Acronyms and Abbreviations

3GPP Third Generation Partnership Project

A-GNSS Assisted Global Navigation Satellite System

AGCH Access Grant Channel

AMLE Approximate Maximum-Likelihood Estimate

BCH Broadcast Channel

BPSK Binary Phase-Shift Keying

BTS Base Transceiver Station

BSC Base Station Controller

BSS Base Station Subsystem

C-RNTI Cell-Radio Network Temporary Identifier

CCCH Common Control Channel

CDF Cumulative Distribution Function

CE Control Element

CEP Circular Error Probable

CF Characteristic Function

CeSAR Cellular Synchronization Assisted Refinement

CoMP Coordinated Multipoint

CRC Cyclic Redundancy Check

CRLB Cramér-Rao Lower Bound

DCCH Dedicated Control Channel

E-911 Enhanced 911

E-CID Enhanced Cell Identification

E-UTRA Evolved UMTS Terrestrial Radio Access

EARFCN E-UTRA Absolute Radio Frequency Carrier Number

eNB enhanced Node B

E-SMLC Enhanced-Serving Mobility Location Center

FCC Federal Communications Commission

FDoA Frequency Difference-of-Arrival

FFT Fast Fourier Transform

GDoP Geometric Dilution of Precision

GPS Global Positioning System

GSM Global System for Mobile Communications

IMSI International Mobile Subscriber Identity

LBS Location-Based Services

LoS Line-of-Sight

LPP LTE Positioning Protocol

LPPM Location Privacy Preserving Mechanism

L1/L2 Layer 1/Layer 2

LFSR Linear Feedback Shift Register

LTE Long Term Evolution

LTE-A Long Term Evolution Advanced

MAC Medium Access Control

MIB Master Information Block

MSE Mean-Squared Error

NLoS Non-Line of Sight

ODTOA Observed Time-Difference-of-Arrival

OFDM Orthogonal Frequency-Division Multiplexing

OFDMA Orthogonal Frequency-Division Multiple Access

PCell Primary Serving Cell

PDCCH Physical Downlink Control Channel

PDCP Packet Data Convergence Protocol

PDF Probability Density Function

PMF Probability Mass Function

PN Pseudo-Noise

PRS Positioning Reference Signal

PSS Primary Search Signal

PUCCH Physical Uplink Control Channel

RACH Random Access Channel

RAR Random Access Response

RF Radio Frequency

RFPM Radio Frequency Pattern Matching

RLC Radio Link Control

RMSE Root Mean-Squared Error

RNTI Radio Network Temporary Identifier

RRC Radio Resource Control

RSRP Reference Signal Received Power

RSRQ Reference Signal Received Quality

RV Random Variable

RX Receive

SCell Secondary Serving Cell

SDCCH Standalone Dedicated Control Channel

SDR Software Defined Radio

SIB Secondary Information Block

SSS Secondary Search Signal

TA Timing Advance

TAG Timing Advance Group

TCH Transport Channel

ToA Time-of-Arrival

TDoA Time-Difference-of-Arrival

TX Transmit

UE User Equipment (i.e., cellular mobile device)

UMTS Universal Mobile Telecommunication System

USRP Universal Software Radio Peripheral

UTDOA Uplink Time-Difference-of-Arrival

WiMAX Worldwide Interoperability for Microwave Access

Executive Summary

Over the past decade, the world has seen a dramatic increase in web-based interconnectedness, which stems largely from the proliferation of cellular technology. Cellular technology's role in connecting mobile users has ushered it into a golden age of relevance in the research community. Cellular technology is thus the focus of network and security researchers alike.

Providing a user location within the context of cellular networks has also long been the subject of study and marketed as location-based services (LBS). The nascence of LBS is such that it has been estimated that the general application of this technology for non-emergency services will generate approximately 15 billion dollars annually [1]. This economic boon has fueled this direction in mobile device location and the creation of the current corpus of research. Applications of LBS include location-sensitive billing, fraud protection, asset tracking, fleet management, surveillance [1], and various other services for autonomous vehicles and wireless networks. Marketing applications also abound, exploiting a user's location for directed advertising and promotions [2]. Finally, as the social fabric of our society extends into digital domains, services like Facebook and Foursquare increasingly leverage LBS to share information about a user's location.

We propose a novel method of passive subscriber geolocation inside a cellular network. Due to the ubiquity of the Long Term Evolution (LTE) standard, we focus specifically on this technology but acknowledge that the methodology could easily be translated to other protocols such as the Worldwide Interoperability for Microwave Access (WiMAX). In the context of LTE, we submit the signaling plane and specifically the timing advance (TA) parameter to this end of user geolocation. This parameter is primarily responsible for managing user mobility in various time division multiple access-based cellular networks. Specifically, this is accomplished via the TA by advancing or retarding a mobile device's uplink transmission time relative to the device distance from the serving base station. In this way, as mobile devices move throughout the serving area uplink collisions resulting in changing propagation delays are mitigated [3]. It is, however, well-known that the TA can be used to estimate mobile equipment distance from serving base stations [4]. Despite this, there is not a rigorous analysis of the best possible positioning accuracy of this method. Additionally, we propose a method of augmenting TA-based positioning,

Cellular Synchronization Assisted Refinement (CeSAR), to further improve the accuracy of TA-based positioning.

CeSAR is an entirely passive method of augmenting TA-based positioning with a simple sensor located in the serving cell. At the heart of CeSAR is the ability to glean additional distance information from the TA by learning when the user is scheduled to transmit an uplink burst. This enables measurement of the time of flight of that uplink burst from the user to the sensor. This information can be combined with the standard user to base station distance traditionally inferred from a TA.

In this work, we examine the TA as a means to position estimation both with and without CeSAR augmentation. We provide new complementary statistical analysis of the TA from which is derived a lower bound on TA-based position estimation. Furthermore, we use this analysis to show how certain parameters of LTE have indirectly resulted in it being possible to provide a consistently accurate position estimate. This has not been possible in older standards such as the Global System for Mobile Communications (GSM). We use simulated and real-world data collected in existing modern LTE networks to validate assumptions about the error distribution of TAs, the lower bound on positioning accuracy, and TA-based positioning accuracy with and without CeSAR augmentation. In these studies, significant attention is given to TA-based geolocation in future heterogeneous networks. Our analysis and field experimentation suggest that accuracies of 40 m to 120 m are possible.

List of References

[1] A.H. Sayed, A. Tarighat, and N. Khajehnouri, "Network-based wireless location: challenges faced in developing techniques for accurate wireless location information," *IEEE Signal Processing Mag.*, vol. 22, no. 4, pp. 24–40, 2005.

[2] I. Güvenç and C.-C. Chong, "A survey on TOA based wireless localization and NLOS mitigation techniques," *IEEE Commun. Surveys & Tutorials*, vol. 11, no. 3, pp. 107–124, 2009.

[3] E. Dahlman, S. Parkvall, and J. Sköld, *4G LTE/LTE-Advanced for Mobile Broadband*. Academic Press, 2011.

[4] C. Drane, M. Macnaughtan, and C. Scott, "Positioning GSM telephones," *IEEE Commun. Mag.*, vol. 36, no. 4, pp. 46–54, 1998.

Acknowledgments

I dedicate this work to my lovely wife, Jessica, whose strength, endurance, and love have not only made this possible but have been the rock on which I have stood throughout it all. From the bottom of my heart, thank you.

To my parents, thank you for unceasing encouragement, support, and unconditional love. These constants have made so much possible.

I would also to thank my advisors Professors Tummala and McEachen. Thank you both for your continuous support. Additionally, I extend a special thank you to Professor Tummala for the endless hours of mentorship, which I will always hold dear.

I also extend my gratitude to my committee members for their continuous support and guidance, and for the dedication of their time to this work.

Finally, I express my appreciation to the following individuals who also contributed to the success of this research: Donna Miller, Anne Pickens, Belinda Proe, Bob Broadston, Allison Hunt, and Alex DeGabriele.

"*Trust in the Lord with all your heart, and do not lean on your own understanding*."

– Proverbs 3:5

THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER 1:
Introduction

Over the past decade, the world has seen a dramatic increase in web-based interconnectedness enabled largely through the proliferation of cellular technology. Cellular technology's role in connecting mobile users has ushered it into a golden age of relevance in the research community. Cellular technology is thus the focus of network and security researchers alike.

The attention cellular technology has garnered from network researchers is fueled by the public's insatiable appetite for faster data rates. Indeed, some estimates project a 1000-fold increase in cellular network capacity over the next several years [1]. Currently, in North America, a LTE subscriber uses approximately 3.7 GB a month. Over the next five years, the average LTE user's data consumption is expected to increase to 22 GB a month [2]. Increasingly, the solution to this capacity demand is centering on the Long Term Evolution (LTE) and LTE-Advanced (LTE-A) protocols as the specific enabling technologies. To wit, LTE subscribers are projected to increase from 1.1 billion in 2015 to 4.3 billion over the next five years [2]. Additionally, LTE-A subscriptions are projected to increase to 500 million by 2018, making massive data rates expected from LTE-A a global reality [3]. Given these projections, it is easy to see why network researchers continue to probe the boundaries of achievable cellular capacity. Due to the prevalence of LTE, we frame our discussion throughout this work in the context of this specific protocol, while acknowledging the potential for the translation of fundamental ideas to other technologies (e.g., Worldwide Interoperability for Microwave Access [WiMAX]).

The burgeoning ubiquity of cellular networks has also been the impetus for research not directly related to increasing capacity. Specifically in the arena of positioning in cellular networks, the Federal Communication Commission's (FCC) E-911 mandate has been especially prevalent in stoking the research [4]. This mandate enables emergency services by requiring cellular operators to provide the location of a cellular device with specific bounds on accuracy. Put forth in a series of phases, the mandate ultimately requires accuracy to within 100 m 67% of the time and 300 m 95% of the time for network-based techniques, and 50 m 67% of the time and 150 m 95% of the time for handset-based techniques [5].

This work in cellular positioning likely served as inspiration for application of this technology in other related areas generically termed location-based services (LBS). LBS is a nascent use of positioning technology; it is estimated that the general application of this technology for non-emergency services will generate approximately 15 billion dollars annually [6]. This economic boon has fueled this direction in mobile device location and the creation of the current corpus of work (e.g., [6]–[10]). Applications of LBS include location-sensitive billing, fraud protection, asset tracking, fleet management, surveillance [6], and various other services for autonomous vehicles and wireless networks. Marketing applications also abound, exploiting a user's location for directed advertising and promotions [10]. Finally, as the social fabric of our society extends into digital domains, services like Facebook and Foursquare increasingly leverage LBS to share information about a user's location.

However, as the cellular market careens towards massive data rates, the market and research community would be wise to consider the second order effects of these technological advances. Specifically, user privacy is an emerging consideration. In the context of LBS, the microcosm of user *location* privacy is of particular interest. Privacy can be defined as [11] "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others." The scope of this definition can be further refined to consider only location privacy as "the ability to prevent other parties from learning one's current or past location" [12]. These definitions subsume ideas many hold about privacy and simultaneously give pause when location data sets are used in applications such as sociological and market studies, optimal cell tower placement, or traffic monitoring [13]. Despite the fact that these data are usually anonymized, it has been shown that that anonymity may not be as strong as previously thought. For instance, remarkable precision has been demonstrated in deanonymization attacks that use computational means such as Markov modeling in attributing specific users to anonymized data [13].

As technology moves forward, preserving these definitions of privacy becomes more obscure and less axiomatic. This difficulty stems from two points. First, the preservation of privacy is obscure because it is nuanced in implementation. One of the main objectives of this work is to demonstrate how privacy is connected in ways that are not directly obvious to seemingly unrelated network parameters. Second, the preservation of location privacy is less axiomatic because users are either not aware of the dangers to their privacy or are

apathetic to these dangers. For instance, one study [14] reported that 250 users willingly turned over two weeks' worth of their driving GPS data in return for a 1 in 100 chance of winning a $200 MP3 player. Furthermore, of the 250 individuals in the study, 97 were asked if their data could be shared with a third party and only 20% refused. The trend indicated by this study is representative of other similar studies [15]–[17].

This work addresses the problem of mobile device location in cellular networks. To this end, we enumerate several objectives framed from two different perspectives: the network operator's perspective and the vulnerability analyst's perspective. First, from the network operator's perspective, we seek a cellular geolocation solution with the following two requirements:

1. An accurate position estimate.
2. A minimal impact on network performance.

The first objective follows as an *ad oculos* requirement since it is obvious that a more accurate position estimate is preferable compared to a less accurate estimate. However, more accurate position estimates usually come at a cost. For instance, in the case of certain positioning schemes that will be detailed later, accuracy may be bought by spending more time training a model [18], [19]. Therefore, rather than search for the most accurate position estimate, we seek the position estimate that is *accurate enough* in light of the second requirement. For instance, in the context of social media, a position estimate that is accurate to within 50 m may be preferable to a position estimate that is accurate to 10 m if the former estimate can be made with no impact to the network performance. To the point, it may be that the latter estimate requires interfacing with the network, perhaps to exchange positioning requests or to send a reference signal. This exchange requires network resources that could otherwise be used for raw data throughput. It is in these scenarios where our solution space lies.

Next, from the perspective of the vulnerability analyst we examine the cellular protocol to the end of evaluating its ability to preserve a user's location privacy. Specifically, we seek to answer the following questions:

1. To what extent is a user's location information leaked in LTE cellular side channels?
2. What is the cost of accessing location information leakage in LTE?

Location privacy and the accuracy of the position estimate are intrinsically linked in that they are at least inversely proportional [20]. This inverse proportionality follows from the fact that as information about a user's whereabouts becomes more accurate that user's privacy necessarily decreases. Thus, as the first question from the security analyst's perspective is answered, the parameters constraining the network operator's first requirement are constructed. We will later show that, in particular, the signaling plane carries a significant amount of location-based information. Moreover, this information is available in plaintext to any passive listener lowering the cost of observation and making the observation reasonably covert.

We then proceed with this dual perspective. In both cases, the most accurate solution is required such that passive observation is still preserved. We begin in Chapter 2 with some necessary preliminaries, such as the wireless channel model that will frame the discussion in the remainder of the work. Chapter 2 then concludes with a survey of modern positioning schemas, including the positioning protocol currently specified by the LTE standard to provide mobile user location. The proposed solution approach is then introduced in Chapter 3. We begin to explore in detail our solution approach in Chapter 4 where we introduce the main mechanism on which our approach will rely, the LTE signaling plane's timing advance (TA) parameter. Chapter 5 then details CeSAR, an entirely passive method by which more information can be gleaned from the TA in order to improve the position estimate. Next, in Chapters 6 and 7, we conduct a rigorous statistical analysis of TA-based positioning. This analysis will reveal an analytical lower bound on achievable performance and show how, with the advent of tighter timing alignment that supports higher data rates, LTE has turned a statistical corner. An indirect result of more strict timing alignment is a much more consistent leak of location-based data than some of the legacy cellular standards like the Global System for Mobile Communications (GSM). The analytical results will then be evaluated in Chapter 8 through the use of synthetic and empirical data. It will be shown that a statistically efficient estimator for TA-based positioning is possible, and expected performance bounds for the proposed scheme will be developed. The present work and major contributions are summarized in Chapter 9 before suggestions for future work are discussed.

The contents of this dissertation have been revised from previous work already published or in publication by the author. Specifically, Sections 2.1, 2.2.4, 2.2.5, 4.8, 5.3, and 8.1.2 are

revised from "Location Privacy in LTE: A Case Study on Exploiting the Cellular Signaling Plane's Timing Advance" by John Roth, Murali Tummala, John McEachen, and James Scrofani to be published in the proceedings of the 50th Hawaii International Conference on System Sciences in January 2017 [28]. Sections 2.3, 4.1–4.6 and 8.1.1 are revised from "Cellular Synchronization Assisted Refinement (CeSAR): A Method for Accurate Geolocation in LTE-A Networks" by John Roth, Murali Tummala, and James Scrofani published in the proceedings of the 49th Hawaii International Conference on System Sciences in January 2016 [24]. Sections 4.7, 6.1, and 6.2 are revised from "Maximum Likelihood Geolocation in LTE Cellular Networks Using the Timing Advance Parameter" by John Roth, Murali Tummala, John McEachen, James Scrofani, and Robert DeGabriele to be published in the proceedings of the 10th International Conference on Signal Processing and Communication Systems in December 2016. Sections 5.1, 6.4–6.9, and 8.3.2 are revised from "On Location Privacy in LTE Networks" by John Roth, Murali Tummala, John McEachen, and James Scrofani which has been submitted for publication.

THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER 2:
Background

In this section, we present the necessary background and review the current state-of-the-art in wireless geolocation. First, we introduce the wireless channel as a necessary preliminary. This is the channel model that the remainder of the background and the main body of presented work itself, will reference. Next, we introduce various methods of positioning in the context of cellular networks. Finally, we introduce the current method of positioning in our target technology, LTE.

This section includes material adapted from work previously published by the author. Specifically, Section 2.1 is revised from "Maximum Likelihood Geolocation in LTE Cellular Networks Using the Timing Advance Parameter" by John Roth, Murali Tumala, John McEachen, James Scrofani, and Robert DeGabriele to be published in the proceedings of the 10th International Conference on Signal Processing and Communication Systems in December 2016 [21]. Sections 2.2.4 and 2.2.5 are revised from "Location Privacy in LTE: A Case Study on Exploiting the Cellular Signaling Plane's Timing Advance" by John Roth, Murali Tummala, John McEachen, and James Scrofani to be published in the proceedings of the 50th Hawaii International Conference on System Sciences [28]. Section 2.3 is revised from "Cellular Synchronization Assisted Refinement (CeSAR): A Method for Accurate Geolocation in LTE-A Networks" by John Roth, Murali Tummala, and James Scrofani published in the proceedings of the 49th Hawaii International Conference on System Sciences in January 2016 [24].

2.1 Channel Model

In this section, we describe the wireless channel mathematically in the context of distance estimation. We pay specific attention to errors associated with standard distance estimation, TA-related error, and non-line-of-sight (NLoS) channels.

In positioning-based models, a common overall representation of the distance relationship

between an anchor point and a position to be estimated is given by

$$\hat{\boldsymbol{d}} = \mathbf{d} + \boldsymbol{\xi} \tag{2.1}$$

where $\hat{\boldsymbol{d}} = [\hat{d}_1, \hat{d}_2, \ldots, \hat{d}_N]^T$ are the observed measured distances from the N base stations, termed in the LTE lexicon enhanced node-Bs (eNBs), $\mathbf{d} = [d_1, d_2, \ldots, d_N]^T$ are the actual distances, and $\boldsymbol{\xi} = [\xi_1, \xi_2, \ldots, \xi_N]^T$ are the set of errors corrupting the true distances. Distance is defined as $d = \| \mathbf{p}_0 - \mathbf{p}_i \|$ where $\| \cdot \|$ is the Euclidean norm and $\mathbf{p}_0 = [x_0, y_0]^T$ is the actual location of the position to be estimated and $\mathbf{p}_i = [x_i, y_i]^T$ is the position of the i^{th} anchor point or base station. We hereafter refer to anchor points exclusively as eNBs and the mobile device whose position will be estimated as user equipment (UE) in keeping with the cellular vernacular. The set of measured distances $\hat{\boldsymbol{d}}$ are then used to determine a position estimate via

$$\hat{\mathbf{p}} = f\left(\hat{\boldsymbol{d}}\right) \tag{2.2}$$

where $f(\cdot)$ is some function making use of available information and $\hat{\mathbf{p}} = [\hat{x}, \hat{y}]^T$ is the position estimate. For our application, $f(\cdot)$ represents a fusion of the observed data in $\hat{\boldsymbol{d}}$.

The noise vector $\boldsymbol{\xi}$ is the source of distance estimation error which virtually guarantees that $\| \mathbf{p}_0 - \hat{\mathbf{p}} \| > 0$, and is of particular interest in all types of wireless positioning. As a first approximation of $\boldsymbol{\xi}$, let

$$\xi_i = \chi_i \tag{2.3}$$

such that $\chi_i \sim \mathcal{N}(0, \sigma_i^2)$ is a normal zero-mean random variable (RV) with some variance σ_i^2. This is typically used to model measurement noise and may be appropriate in some channel conditions, for example, if a line-of-sight (LoS) condition exists between the transmitter and receiver [7]. LoS conditions imply that there are no physical obstructions between the transmitter and receiver in the wireless channel. Common applications of this simplified noise model include the global positioning system (GPS) and rural multilateration.

Next we expand on (2.3) in order to describe a $\boldsymbol{\xi}$ that is tailored to errors associated with TA-based ranging measurements. The TA is a control plane parameter used by the network to take into account propagation delay between a UE and eNB when synchronizing the

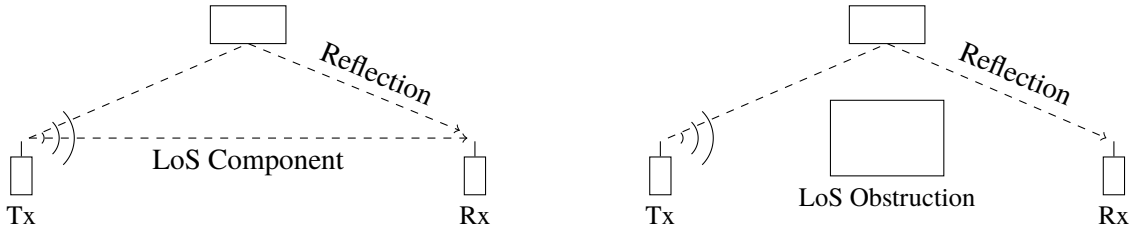


Figure 2.1. The difference in a multipath and NLoS channel

UE's uplink burst[1] [22]. The TA is a discrete quantity, thus the error associated with the TA ranging measurement is classically approximated as essentially a quantization noise term. Specifically, in LTE, the TA has a quantization interval of 78.125 meters [23], [24]. Therefore, under this ideal model, error can be modeled as

$$\xi_i = \omega_i \tag{2.4}$$

where ω_i is the quantization error associated with the i^{th} TA measurement error. This simplification of TA-based error is nuanced, and thus, a significant body of the present work is dedicated to bringing to light the conditions under which this assumption can be made. Commonly, this error is modeled ideally as a uniformly-distributed RV [24]–[26]. However, for realistic applications, this model alone may not hold. Research in GSM and LTE networks has shown that the TA may be more accurately modeled by a normal distribution [27]–[29] or approximately normal distribution [21], as described by

$$\xi_i = \chi_i + \omega_i \tag{2.5}$$

which is consistent with the empirical data presented in this work (cf. Chapter 4). This indicates that the TA transition areas are not hard transitions as commonly assumed, but rather have fuzzy boundaries or transition zones. This can be explained by time-varying channel conditions as well as errors associated with distance estimation at the eNB (which is ultimately responsible for calculating the UE distance and issuing a TA).

In some use cases, the error cannot be accurately modeled by (2.5) either. For instance,

[1]Further analysis of the inner workings and details of the TA will be the exclusive subject of a subsequent chapter.

in physically dense environments (e.g., urban canyons), the channel is often polluted by buildings, skyscrapers, and the like, which obstruct the LoS from the UE to the eNB. At the very least, this results in a multipath scenario, shown in the left pane of Figure 2.1. In multipath propagation, the signal arrives at the receiver via at least one reflected path, which will travel some non-minimal distance. There may be a LoS component; however, it is not guaranteed to be the strongest of the arriving signal components. For instance, two reflected paths may add constructively at the receiver to provide a combined signal strength larger than that of the LoS component. In severe cases, there will be no LoS component, as in the right pane of Figure 2.1, and the channel can be described as non-line of sight (NLoS). In these scenarios, the distance error will always be positively biased, since all signal paths travel some non-minimal distance, and the noise model can be extended such that

$$\xi_i = \chi_i + \omega_i + \eta_i \tag{2.6}$$

where η_i is some positively-biased RV representing the error associated with NLoS conditions between the UE and the i^{th} eNB. Popular models for η include an exponential distribution [30], a uniform distribution [31], a positively-biased normal distribution [7], [27], [30], and a Rayleigh distribution [30]. Common applications of this NLoS noise model include positioning in dense urban environments or indoor scenarios.

Given (2.6), $\boldsymbol{\xi}$ is a random vector where the probability density function (PDF) of each element is the result of a double convolution

$$p_\Xi(\xi_i) = p_X(\chi_i) * p_\Omega(\omega_i) * p_N(\eta_i). \tag{2.7}$$

Depending on what distribution types are used for each RV a closed-form solution for $p_\Xi(\xi)$ may not be possible. For now we leave these distributions as generically defined and later ascribe specific distribution types to them.[2]

2.2 Approaches to Positioning

In this section, we provide a brief taxonomy of relevant traditional techniques in wireless localization. We then provide a review of previous work in TA-based positioning. For

[2]This section was revised from [21].

the purposes of our taxonomy, the positioning system will consist of several eNBs whose positions are known and a target to be located. Additionally, the target is assumed to be emitting a radio frequency (RF) signal with known content and transmit power.

2.2.1 Multilateration

The first class of positioning solutions in our taxonomy is multilateration. In this solution approach, the distance of the target is estimated from several eNBs. Those distance estimates are then fused into a position estimate via some nonlinear function, $f(\cdot)$. The first of the multilateration-based techniques measures the received signal strength (RSS) from multiple eNBs. Because the strength of the signal is known *a priori*, a path loss model is used to estimate the eNB-target distance. This received signal strength model leans heavily on an exact known broadcast strength and an accurate model of the path loss $\mathcal{L}$ [7], [8] classically described by

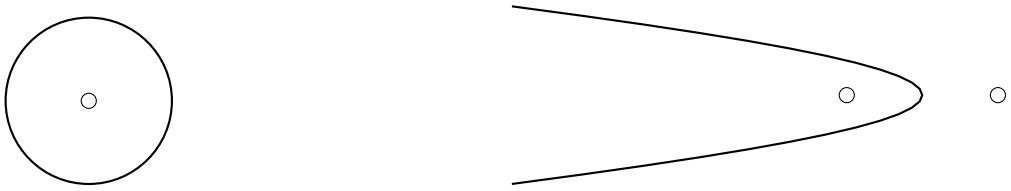
$$\mathcal{L} = \gamma 10 \log \left(\frac{4\pi d}{\lambda} \right) \tag{2.8}$$

where d is the is the propagation distance, the path loss exponent γ models the propagation environment, and the wavelength λ is set by the transmit frequency.

A position can also be estimated through multilateration via time-of-arrival (ToA) calculation. This solution leverages knowledge of the signal's time of flight and propagation speed to calculate the eNB-target distance to produce a circular locus such as that shown in the left pane of Figure 2.2. Because this technique is highly sensitive to variations in time, it assumes a very precisely synchronized system. Notably, not only do the eNBs need to be synchronized in time, but the target must also be synchronized [7], [8]. The position estimate is then made by some means from the resulting system of equations

$$\begin{aligned} (x - x_1)^2 + (y - y_1)^2 &= \hat{d}_1^2 \\ (x - x_2)^2 + (y - y_2)^2 &= \hat{d}_2^2 \\ &\vdots \\ (x - x_N)^2 + (y - y_N)^2 &= \hat{d}_N^2 \end{aligned} \tag{2.9}$$

which, if any error is present, will likely be inconsistent for $N > 2$ eNBs or underdetermined for all other N.



(a) ToA & RSS (b) TDoA & FDoA

Figure 2.2. The locus geometry for different multilateration-based positioning schemas. Note that for the TDoA and FDoA techniques, $N-1$ loci are produced while in ToA and RSS N loci are realized.

The final solution to multilateration is time-difference-of-arrival (TDoA). This technique uses the time *difference* of arrival to calculate the position estimate. In this way, the signal's absolute time of flight is not needed, rather only the differences in time of flight is required. These measurements result in hyperbolic loci where the eNBs are the foci of the hyperbolae described by

$$\left((x-x_i)^2+(y-y_i)^2\right)-\left((x-x_j)^2+(y-y_j)^2\right)=\Delta\hat{d}^2_{\{i,j\}} \quad \forall\, i,j \quad i\neq j. \tag{2.10}$$

One main advantage of this technique over the ToA technique is that, while the eNBs still require strict time synchronization, the target need not be synchronized [7], [8][3]. On the other hand, TDoA will always produce one less equation in (2.10) than in (2.9), thus while a minimum of $N=3$ eNBs are required for a two dimensional fix with ToA, $N=4$ eNBs is required for a two dimensional fix with TDoA

One notable limitation of multilateration techniques is that they assume the RF signal is transiting the minimal transmitter-receiver distance. As we have seen in a multipath environment, and especially NLoS channels, this may not be the case. Therefore, the performance of these techniques is additionally tied to the assumption of a LoS channel. This assumption will not hold in some channels which include indoor and dense urban environments.

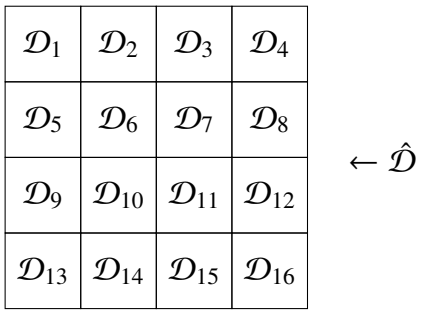


Figure 2.3. The database correlation method of positioning where a radio signature $\hat{\mathcal{D}}$ is compared to database elements $\hat{\mathcal{D}}_i$ collected *a priori* at certain locations. The location at which the closest database element match was taken is used as the position estimate.

2.2.2 Database Correlation

A popular alternative to multilateration methods is the database correlation technique (also known as "fingerprinting" or "radio frequency pattern matching"). This technique seeks to leverage spatial diversity in a multipath environment to improve positioning. To this end, radio signatures are collected at various locations and stored in some database $\mathcal{D}$. Signatures that have been previously used and demonstrated as effective include the channel impulse response [33], [34], the RSS [19], [35], observable cell IDs [18], [36], [37], and network parameters such as the TA [38], [39]. This database of radio signatures is then compared with measurements made online, $\hat{\mathcal{D}}$. The location at which the closest database match was taken is used as the position estimate. While the database correlation method can be robust in multipath environments, it has a large database creation (i.e., database training) and maintenance cost [18], [19]. Additionally, it is easy to see that accuracy can be tied to database size. Thus, as more accuracy is desired a more granular database must be created and maintained. Also, as the database size grows, the computational cost associated with the database search increases.

2.2.3 Timing Advance-Based Positioning

As TA-based positioning is at the center of this work, we now provide a review of previous TA-based research. This literature survey was previously presented in [28]. The TA has long been studied as a means to positioning and can be seen as specific cases of multilateration or

[3]A close relative of TDoA is frequency difference-of-arrival (FDoA) where Doppler shift is used in conjunction with eNB-target relative motion to describe a hyperbolic system of equations [32].

even as database correlation. The TA can provide a rough eNB-target distance measurement such that ToA techniques can be applied to this specific type of measurement. Additionally, as will be shown in a subsequent section, the TA has also been used as a radio signature in fingerprinting databases [39].

2.2.4 The Timing Advance in GSM

The investigation of the TA for positioning applications began before the advent of LTE in GSM, a legacy protocol. For instance, in [40], the authors discuss the possibility of using the GSM TA as a mechanism for positioning. They note poor accuracy and suggest forcing base station handovers in order to get a second TA to improve positioning. They conclude that the accuracy is not sufficient for TA to be seriously considered by itself as a method for positioning.

Accuracy concerns are echoed in [5] where it is estimated that the accuracy of the GSM TA is theoretically 550 meters and practically 2,200 meters. Nevertheless, it is noted that a cell tower, termed base transceiver station (BTS) in GSM, location in conjunction with the TA is used in many countries around the world as a means for subscriber localization. This is also a "fallback" GSM localization technique in the United States if a subscriber cannot be located with other, more accurate, means.

The authors in [25] suggested taking multiple TA measurements from the same tower and averaging them in order to improve distance estimation. An analysis of the method is presented, but no real-world experimentation was conducted. It was noted that their method will only result in a distance from the BTS, and any further improvement in accuracy will be the fruit of other means.

In [41], the authors propose the use of GSM TA for traffic state estimation, not for precise user localization. However, their evaluation oversimplifies the TA behavior in simulation. Similar to the other studies described thus far, no empirical data are used.

The authors in [26] present the only study we are aware of that uses empirical TA data observed from a GSM network; however, their application was in finding GSM BTSs and not user location. Their study was still largely simulation based, and they only presented

one real-world example.[4]

2.2.5 The Timing Advance in LTE

The largely unsuccessful first forays into using the TA as a parameter for localization are probably to blame for the limited amount of research in GSM TA-based positioning. With an accuracy as low as 550 meters to 2.2 kilometers [5], it is not surprising that the TA did not receive much attention in the literature initially.

It was not until Jarvis et al. [23] recognized the potential in the TA parameter in LTE networks that researchers reopened their study of the TA as a means to positioning. Although again a simulation-only approach, the authors showed viable positioning accuracy in three dimensions when using a TA from three and four eNBs. The authors did not address how using more than one eNB would be possible nor did they assume there was any error associated with the eNB in issuing the correct TA to the UE. Similar investigations were conducted using WiMAX technology in [42].

In [38], Wigren uses the LTE TA as a complementary database feature when performing localization via fingerprinting. Using a heuristic approach to modeling the behavior of the TA, he noted accuracies on the order of his TA error and suggested his algorithm as an appropriate fallback technology for positioning for E-911 in LTE if Assisted GPS was not available.

The authors in [43] used LTE TA as a means for proximity discovery in device-to-device communications. They showed through simulation that errors as low as 50 meters were possible for certain eNB geometries. However, their modeling of the TA was also heuristic, and did not account for any error in the eNB issuing an incorrect TA.

The work represented by [44] is the only published work we are aware of that uses empirical measurements to validate TA-based positioning approaches in LTE. Their approach did not, however, focus on characterizing the TA. Rather, similar to Wigren's approach, they used it as another feature in a fingerprinting approach to localization with the aim of minimizing the cost of training their fingerprint database. They also made no attempt to characterize how the TA value correlated with the true distance of the UE.

[4]This section was revised from [28].

In summary, the corpus representing the TA parameter in the literature is conspicuously sparse. Even more absent are studies conducted with empirical data, thus making modeling in simulation largely a product of conjecture. [5]

2.3 LTE Positioning Protocol

In this section, we describe how the network currently provides LBS to the UE in LTE. This is done via the LTE Positioning Protocol (LPP) [39]. LPP allows for several methods of position location: Observed Time-Difference-of-Arrival (OTDOA), Assisted Global Navigation Satellite System (A-GNSS), and Enhanced Cell ID (E-CID).

A-GNSS is well studied and provides very reasonable accuracy. With the integration of the required hardware in many modern mobile devices, A-GNSS arises as an adept solution to the mobile location problem. Despite this, there still exists a legacy population without the required hardware that must be serviced. Additionally, A-GNSS usually comes at a high power cost which, given the power-constrained mobile platform, is undesirable. Finally, the emerging requirement for accurate positioning indoors and in metropolitan canyons requires an alternative solution [45].

OTDOA is a positioning method where a UE will measure the time difference of arrival of the LTE Positioning Reference Signal (PRS) from multiple eNBs. This information is then sent to a network-based Enhanced Serving Mobile Location Center (E-SMLC). With three or more eNBs, the resulting system of equations can be solved to provide a position estimate. However, like A-GNSS, OTDOA suffers in urban and indoor environments where NLoS and multipath channels dominate. Release-11 will complement OTDOA with Uplink Time-Difference-of-Arrival (UTDOA). The main difference being that UTDOA is determined by the eNBs after a signal is sent from the UE [45] whereas the opposite is true in OTDOA.

The third method enlisted by LPP for UE positioning is enhanced-cell ID (E-CID). This method is identical to the database correlation method. When a UE initiates an LPP session, and E-CID is the chosen method from which to derive a position, the network will negotiate with the UE which radio signatures the UE will measure and send to the E-SMLC to be compared against its database. This measurement set is reliant on the composition of the

[5] This section was revised from [28].

a priori database and the UE capabilities. Measurements specified in the LPP standard include cell-ID, reference signal received power (RSRP), reference-signal received quality (RSRQ), and TA [39]. The best radio signature set useful for positioning is currently an open topic (e.g., [38]); however, data fusion has been suggested by the body governing the development of LTE, the Third Generation Partnership Project (3GPP), [46] via

$$\hat{\mathbf{p}} = \arg\min_{\mathbf{p}} \frac{\| \hat{\mathcal{D}}_{\text{RSRP}} - \mathcal{D}_{\text{RSRP},i} \|}{\sigma^2_{\mathcal{D}_{\text{RSRP},i}}} + \frac{\| \hat{\mathcal{D}}_{TA} - \mathcal{D}_{\text{TA},i} \|}{\sigma^2_{\mathcal{D}_{\text{TA},i}}} \tag{2.11}$$

where $\hat{\mathcal{D}}_{\text{RSRP}}$ is the UE measured RSRP, $\mathcal{D}_{\text{RSRP},i}$ is the i^{th} pre-recorded RSRP measurement, $\hat{\mathcal{D}}_{\text{TA}}$ is the current UE TA, $\mathcal{D}_{\text{TA},i}$ is the i^{th} pre-recorded TA measurement, and $\sigma^2_{\mathcal{D}}$ are the respective database variances. Here the variances have been included as weights to normalize the effect of datasets with different statistics.

Finally, it should be noted that LPP sessions are ciphered [47] and, as such, effectively protected data. This study assumes these data to be unreadable and thus not available for exploitation.[6]

[6]This section is revised from [24].

THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER 3:
Solution Approach

In this work, we propose a novel method to localize a connected cellular device based on the LTE signaling plane TA parameter. While this work specifically focuses on applications in LTE/LTE-A, the fundamental process is applicable to all cellular technologies which manage mobile device timing alignment (e.g., WiMAX).

As was seen in the literature survey in Chapter 2, it is well-known that, in addition to maintaining time alignment, the TA can be used to estimate UE distance from serving eNBs [23], [40]. However, there is not a rigorous analysis of the best possible positioning accuracy of this method. We will show through analysis how, with the advent of tighter time alignment in LTE, the TA has turned a statistical corner making positioning a UE with an unprecedented level of *consistent* accuracy possible. Additionally, we propose a method of augmenting TA-based positioning to further improve accuracy. Referring now to Figure 3.1, we outline the proposed scheme in three general steps. First, relevant data are collected. Primarily, this includes TA data sent to the target UE from which a distance estimate is inferred. Optionally, the TA data are then augmented with the CeSAR algorithm. The position estimate is then made with the resulting data set.

3.1 Data Collection

Data collection begins with initialization with the relevant parameters that are assumed to be known *a priori*. The parameters in question include the serving eNB location(s), the cellular address of the UE to be located, the operating E-UTRA absolute radio frequency carrier number (EARFCN), and each eNB's TA bias[7]. The mobile UE is uniquely identified with an international mobile subscriber identity (IMSI), which the network maps to a cellular software address. This software address must be known in order to ascribe the correct TA values to the UE since a multiplicity of UEs may receive TAs from a single eNB. The geometry of the serving eNB(s) can be ascertained directly by site survey or by statistically

[7]It should be noted that in practical scenarios involving a sectored eNB, the UE sector must also be known in order to ensure the third party can receive information transmitted from the tower to the UE. In this work, we assume that eNBs are not sectored.

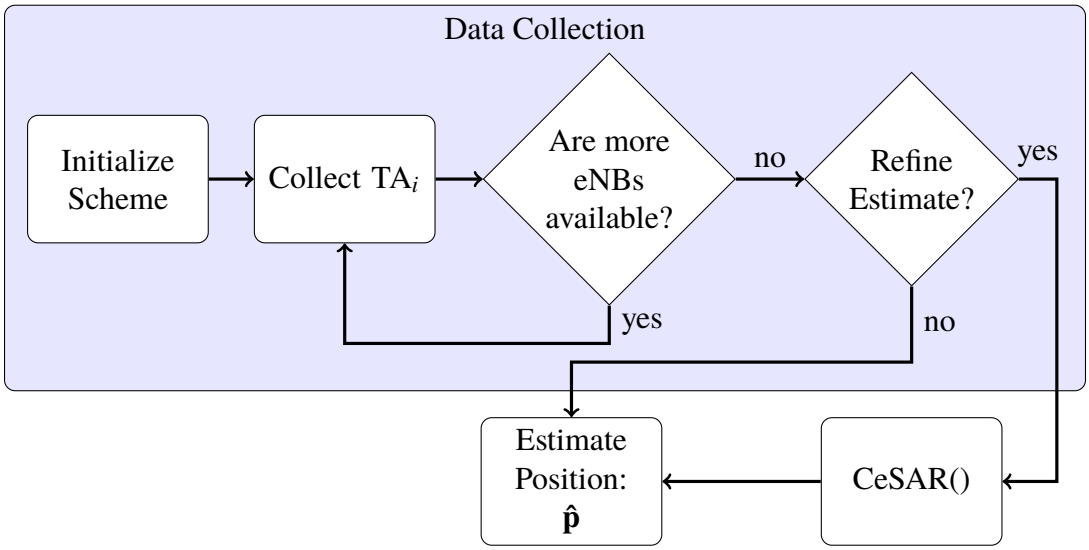


Figure 3.1. The proposed scheme for TA-based positioning

inferring eNB locations from data collected in the field (i.e., war driving) [26]. We assume the former in order to not confound the major sources of error. Finally, in practice, we find that each eNB has its own specific TA bias which must be known *a priori* in order to achieve an unbiased position estimate. This bias can be measured directly during site surveys.

Next, TA data issued from the network to the target UE are collected. If more than one eNB is serving the UE (a type of physically disjoint carrier aggregation) this collection is repeated for each of the $N > 1$ eNBs. As cellular technology evolves to embrace the idea of heterogeneous networks (i.e., LTE-A release 11+), the scenario where $N > 1$ becomes more realistic, drastically improving the quality of a position estimate.

Once a TA from each serving eNB is collected, the option to refine the estimate further is or is not exercised. In order to simplify the analysis, we focus specifically on the case of localization and not tracking. In other words, prior information is not used to improve the current position estimate (e.g., Markov or Kalman filtering). Rather, one TA collection is used to perform a static position estimate of the target UE. The number and geometry of serving eNBs will later be shown to heavily influence the positioning accuracy. More eNBs will generally produce a more accurate estimate. The effect of the eNB geometry on the position estimate is more difficult to dilute into a rule of thumb. However, in general terms, the more eNBs that are collinear or approximately collinear generally reduces precision.

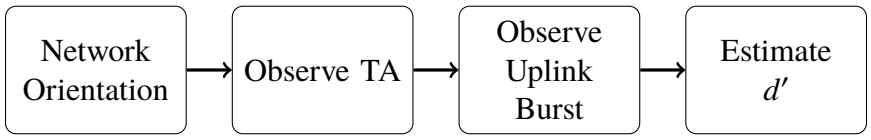


Figure 3.2. The CeSAR algorithm

Positioning can be done from several frames of reference: the network, mobile, or third party. If the positioning is network-centric then the eNBs will communicate TAs issued back to a central server which will perform the position estimate of the target UE. If the positioning is mobile-centric, then the UE collects all issued TAs and performs the position estimate locally. In both of these cases it is trivial to acquire both the local eNB geometry, UE address, and eNB bias since it is reasonably assumed that the network both knows these parameters and will be cooperative. Alternatively, if the positioning is done by third party, the TAs will be observed over the air[8] and the sensor can report its measurement in any number of ways to the third party. Because scheme initialization is non-trivial from a third-party viewpoint and thus the most arduous frame of reference to take, we hereafter assume this perspective.

3.2 Cellular Synchronization Assisted Refinement

If the option to refine the estimate is exercised, then the CeSAR algorithm [24], presented in Figure 3.2, is used. Notably, the algorithm requires input from an extra-network sensor. This sensor can be implemented with a relatively cheap software defined radio (SDR) solution and is detailed further in a later chapter. Ultimately, the algorithm adds an extra dimension to the existing TA-only system of equations and therefore has less error than the distance estimate provided by the TA(s) alone. This augmented system of equations is then later used to estimate the target UE position.

CeSAR begins by orienting the sensor to the network by observing cellular network beacon signals. These signals communicate network organizational information which includes frame boundary locations in time. This synchronization enables the sensor to perform further demodulation and observation of network traffic. After the sensor is oriented, it observes a TA issued to the target UE from a serving eNB. From this information, the sensor determines both when the UE is instructed to transmit its next uplink burst and the target

[8]The TA will later be shown to be sent unencrypted, making this type of observation possible.

UE's approximate distance from the eNB. Finally, the sensor estimates its distance to the target UE d' by calculating the time of flight of a UE uplink burst to the sensor.

This technique of augmentation has several advantages, foremost of which is that the augmentation is performed entirely passively. Because the sensor is not required to transmit during any portion of the augmentation it simultaneously makes the process impossible to detect from electromagnetic emanation and does not offer any further traffic load to the network. Furthermore, all information utilized in the refinement process is sent in plaintext, thus it does not require the sensor to bypass encryption. Additionally, strategic positioning of the sensor can overcome geometric dilution of precision (GDoP). Because control of the network geometry is usually not possible, this point is significant and is demonstrated further in the work.

For the aforementioned reasons, we submit that the proposed method of augmentation is preferable from a network operator perspective and simultaneously attractive from a vulnerability analyst's perspective. Because the additional required infrastructure (i.e., sensor) is inexpensive and, in contrast to LPP, it does not offer further network load it is an attractive solution to network providers seeking to maximize network performance while minimizing operational costs. Alternatively, it is also a significant finding from a vulnerability analyst's perspective, because it is a passive technique that can be utilized relatively covertly.

3.3 Position Estimation

Once the data are collected (regardless of whether they are augmented with CeSAR) the position estimate can be made as in Figure 3.3. A benefit of the proposed scheme is that there is no requirement on the resulting system of equations (e.g., consistency, overdetermined, underdetermined, etc.). Specifically, the estimate is calculated through a nonlinear programming approach parameterized by the latent distributions of error which seeks the *most likely* position of the UE. The type of position estimate is termed the maximum-likelihood estimate (MLE).

When developing a MLE a critical first step is understanding the underlying error distributions associated with the measurements. This is perhaps the most crucial step, since the

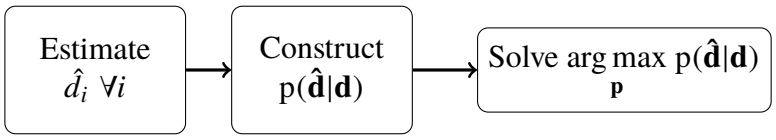


Figure 3.3. The method of position estimation

final position estimate is only the *most likely* position location if the error distribution is well understood. We will later cast the TA error as a quantized RV and show that the error can be modeled as normally distributed. Thus, the MLE of the true distance from a distance estimate that is normally corrupted $\hat{d}_i$ for a single measurement is the measurement result itself. This straightforward result hinges on the assumption made about the underlying error itself. However, the underlying phenomenon associated with a TA is complex, therefore, a significant amount of work is dedicated to substantiating the claim for latent normality.

After $\hat{d}_i \ \forall i$ is established, if measurements are CeSAR-augmented, the vector of all $\hat{d}_i$ is concatenated with the CeSAR measurement $\hat{d}'$. Explicitly, the resulting vector of measurements used to perform the position estimate is either $\hat{\boldsymbol{d}} = [\hat{d}_1, \ldots, \hat{d}_N]^T$ if augmentation is omitted or $\hat{\boldsymbol{d}} = [\hat{d}_1, \ldots, \hat{d}_N, \hat{d}']^T$ if augmentation is implemented. Those N or $N+1$ measurements are then used to construct an error surface defined by the conditional probability density function $p(\hat{\boldsymbol{d}}|\mathbf{d})$.

Finally, finding the *most likely* position requires finding the argument $\mathbf{p} = [x, y]^T$ which maximizes the error surface $p(\hat{\boldsymbol{d}}|\mathbf{d})$ via the program

$$\hat{\mathbf{p}} = \arg\max_{\mathbf{p}} p(\hat{\boldsymbol{d}}|\mathbf{d}). \tag{3.1}$$

For some distributions, finding the exact MLE requires an exhaustive search over all $\mathbf{p}$ [10]. Because of the non-trivial computational burden levied by such a brute force approach, significant effort has been made in the research to find approximate solutions to this maximization program (e.g., [31]). Because this problem is well-traveled in the literature, it is not a focus of this work. Instead, we use computationally intensive means to arrive at $\hat{\mathbf{p}}$ in order to avoid idiosyncrasies associated with some of the more nuanced solutions in the literature.

3.4 Performance Metrics

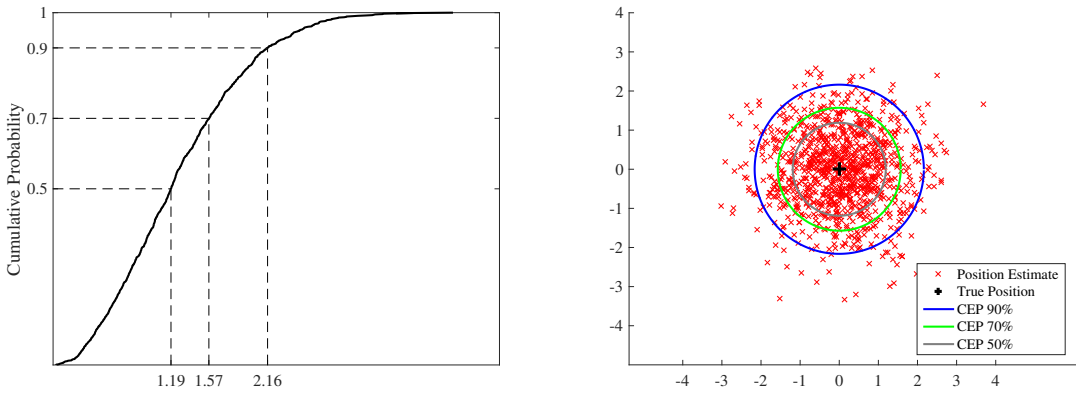
The Cramér-Rao Lower Bound (CRLB) is a well-accepted lower bound on the performance of an unbiased estimator [10], [48]. However, like the MLE, the CRLB is highly dependent on understanding the distribution of the underlying error. Additionally, the CRLB can be difficult to calculate in closed form for certain non-standard error distributions [21]. Despite the fact that the error associated with a TA is a discrete RV[9] and thus strictly non-injective in terms of the observed rounded RV, we will show that the CRLB can be derived through an understanding of the RV through the lens of quantization. The values realized by evaluation through the CRLB are also somewhat abstract as they are given in mean-squared error (MSE) or root mean-squared error (RMSE). In both cases, the errors are squared before the mean is taken (in the case of RMSE the root of the mean is then taken) via

$$\begin{aligned} \text{MSE} &= \sum_{i=1}^{N} \|\mathbf{p}_0 - \hat{\mathbf{p}}_i\|^2 \\ \text{RMSE} &= \sqrt{\sum_{i=1}^{N} \|\mathbf{p}_0 - \hat{\mathbf{p}}_i\|^2} \end{aligned} \tag{3.2}$$

for N trials and $\|\cdot\|$ is the Euclidean norm. Of these two abstract metrics, RMSE provides values that are most easily understood. While the RMSE cannot be directly translated to mean error, the values are the most intuitively satisfying.

While we rely primarily on the CRLB to show theoretical lower bounds on the performance, accuracy is also demonstrated in specific cases with the circular error probable (CEP). CEP is established in context of a certain percentage. For example, CEP 70% will result in a distance within which the error associated with $\hat{\mathbf{p}}$ will fall with probability 0.7. To further illustrate the contribution of this metric we present a case study in Figure 3.4. In this figure, a UE is located at $\mathbf{p}_0 = [0, 0]^T$ and successive position estimates are made which are corrupted by independent and identically distributed normal measurement noise in both the orthogonal Cartesian directions. In the left pane of the figure, a cumulative density function (CDF) representing the error associated with the position estimate is shown. The CDF describes the probability that a realization of a RV X will fall below a given value x

[9]The TA can be seen as a rounded distance measurement; see Chapter 4 for further treatment of the TA.



(a) (b)

Figure 3.4. The circular error probable at 50%, 70%, and 90% shown with a CDF and in simulation

via [49]

$$F_X(x) \equiv \Pr[X \leq x] = \int_{-\infty}^{x} f_X(y)dy \tag{3.3}$$

where $F_X(\cdot)$ is the CDF and $f_X(\cdot)$ is the PDF defined by [49]

$$f_X(x) = \frac{d}{dx}F_X(x). \tag{3.4}$$

The values of x for $F_X(x) = \{0.5, 0.7, 0.9\}$ are all shown on the x-axis in the left pane of Figure 3.4 and can be interpreted as the distance from the true position that a certain percentage of the estimates $\hat{\mathbf{p}}_i$ will fall. For instance, in the case of the study presented in Figure 3.4, 70% of all position estimates will fall within 1.57 units of $\mathbf{p}_0$.

While CEP gives a more intuitive metric, it is most useful in Monte-Carlo simulation with more complex underlying errors and cannot usually be derived analytically. Additionally, we sometimes present the empirical moments from a simulation along with CEP in order to provide a more complete statistical picture. However, the empirical moments do not necessarily align with the CEP metric. In other words, if X_1 and X_2 are both RVs it could be that X_1 has a lower CEP 70%, but X_2 has a lower mean error.

3.5 Summary

The proposed scheme has several distinct advantages and limitations. In contrast to TA-based resolution in legacy networks, the scheme is accurate on the order of tens of meters. However, the accuracy is proportional to the number of available eNBs N so, in the common legacy case where $N = 1$, accuracy suffers somewhat. Nonetheless, as cellular infrastructure evolves, it is expected that the case where $N > 1$ will become increasingly common [3] lending itself to multiple eNB positioning. With augmentation, accuracy can also be improved on the order of tens of meters and without the need for any emissions from the augmentation sensor (i.e., passively). This makes CeSAR augmentation a sensible choice for heavily congested networks and applications requiring discretion since it does not add traffic to the existing network. An obvious limitation is that it requires extra hardware to be introduced into the network.

In the subsequent chapters, we detail the efficacy of the proposed solution approach through a thorough treatment of data collection, CeSAR augmentation, and position estimation.

CHAPTER 4:
Morphology of the LTE Timing Advance

In this section, we present a review of the LTE standard with the specific focus of the structure and relationship of the TA to the protocol at large. The operation of the TA in current (legacy) network deployments and future (heterogeneous) deployments is discussed.

This chapter includes adaptations from work which has been previously published by the author. Specifically, sections 4.1-4.6 are taken from "Cellular Synchronization Assisted Refinement (CeSAR): A Method for Accurate Geolocation in LTE-A Networks" by John Roth, Murali Tummala, and James Scrofani published in the proceedings of the 49th Hawaii International Conference on System Sciences in January 2016 [24]. Section 4.7 is revised from "Maximum Likelihood Geolocation in LTE Cellular Networks Using the Timing Advance Parameter" by John Roth, Murali Tummala, John McEachen, James Scrofani, and Robert DeGabriele to be published in the proceedings of the 10th International Conference on Signal Processing and Communication Systems in December 2016 [21]. Section 4.8 is revised from "Location Privacy in LTE: A Case Study on Exploiting the Cellular Signaling Plane's Timing Advance" by John Roth, Murali Tummala, John McEachen, and James Scrofani to be published in the proceedings of the 50th Hawaii International Conference on System Sciences in January 2017 [28].

4.1 Time Alignment Management in LTE

The TA is a signaling plane parameter with the purpose of reconciling UE mobility with quality of service. LTE uses an orthogonal frequency-division multiple access (OFDMA) scheme which requires that transmissions are highly disciplined in time and frequency in order to avoid intersymbol interference with other UEs sharing service with the same eNB [22]. As UEs move throughout a serving cell their distance to the serving eNB may change thus changing the propagation delay between the UE and the eNB. The eNB constantly estimates the UE-eNB distance and issues TA updates in order to ensure the UE is continuously synchronized in time relative to the propagation delay.

Ever since GSM, the TA quantity has been recognized as useful for positioning cellular

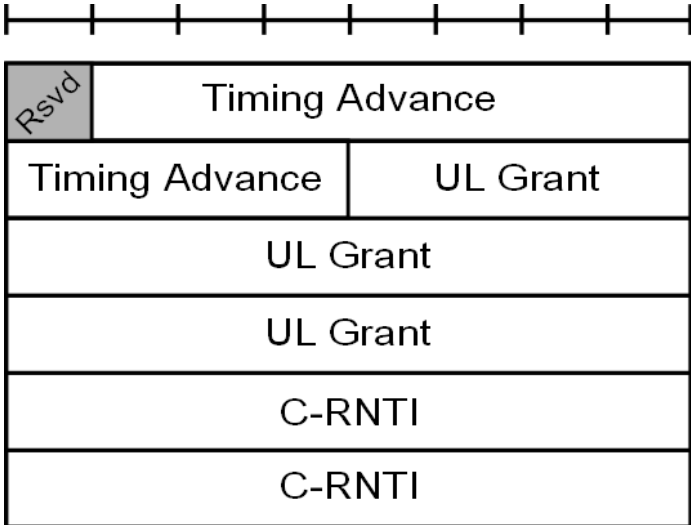


Figure 4.1. The random access response (RAR) message found in the media access control (MAC) header. Bit boundaries are denoted by the bar above the figure. Adapted from [50].

devices [23], [40]. In this section we aim to develop context for the TA inside LTE networks.

The TA takes two forms during normal cellular operation. The first is the TA that is negotiated during the initial network random access. After the UE has obtained downlink synchronization via the primary and secondary search signals (PSS/SSS) and the corresponding system information from the master and system information blocks (MIB/SIB) the UE requests network access from the eNB via a random access preamble. If the request is successful the eNB continues network access negotiation with a random access response (RAR) message. As seen in Figure 4.1, inside this message is the cell radio network temporary identifier (C-RNTI)[10], an uplink resource grant, and an 11-bit TA quantity where $T_A \in \{0, 1, \cdots, 1282\}$ [50]. This quantity directs the UE to begin transmission of its uplink frame $16 \times T_A \times T_s$ seconds *before* the beginning of the corresponding downlink frame, where T_s is the sampling frequency [51], [52].

The second form the TA takes is during normal maintenance of the eNB-UE connection. Unlike the TA during initial network access, this TA only adjusts the UE's uplink timing based on its current timing and is thus relative. As the mobile device moves throughout the vicinity of the eNB its distance to the eNB will likely change. In order to maintain the uplink

[10]This is a temporary user address which will receive further discussion in Section 4.3.

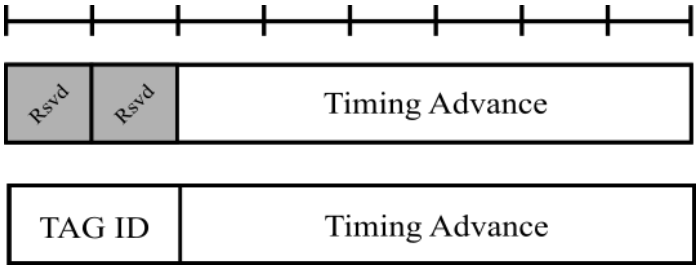


Figure 4.2. The legacy timing advance command (top) and the release 10+ timing advance command (bottom). Bit boundaries are denoted by the bar above the figure. Source: [50].

timing alignment, the eNB will periodically issue TA commands to the UE. These six-bit TA commands come in the form of a medium access control (MAC) control element (CE) as seen in Figure 4.2 [50]. Because only six bits are used $T_A \in \{0, 1, \cdots, 63\}$. Each command moves the UE's current uplink timing by $16 \times (T_A - 31) \times T_s$ seconds. The possibility of a negative value allows for the uplink timing to be advanced or retarded depending on which direction the UE is moving relative to the eNB [51], [52].

Additionally, as of Release 9, type 1 and type 2 TAs are introduced [53]. A type 2 TA is determined by the eNB via the UE generated random access preamble and calculated as

$$TA_2 = \hat{t}_{eNB,Rx} - \hat{t}_{eNB,Tx} \tag{4.1}$$

where $\hat{t}_{eNB,Rx}$ is the time instance where the eNB receives the UE random access preamble as determined by the first path and $\hat{t}_{eNB,Tx}$ is the standard eNB frame timing. A type 1 TA is calculated during the maintenance phase via

$$TA_1 = (t_{eNB,Rx} - t_{eNB,Tx}) + (t_{UE,Rx} - t_{UE,Tx}) \tag{4.2}$$

where the first difference is the time separation between a received uplink frame and its transmit timing and the second difference is the time separation of those same frames only this time at the UE. The second difference is always positive, while the first may be positive or negative. The type 1 TA theoretically allows the eNB to determine the round trip time with arbitrarily small error and use this to advance or retard the served UE's uplink timing. It should be noted that the type 1 TA is never sent over the radio link and is thus not available for exploitation over the air by a third party; however, we later discuss how a passive listener

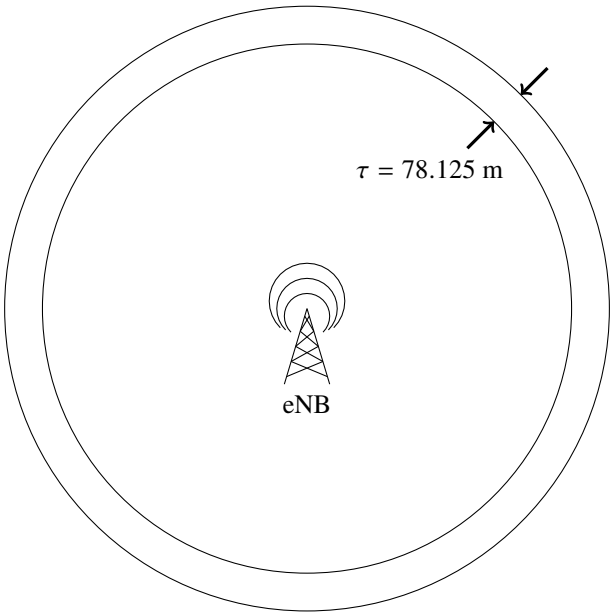


Figure 4.3. The uncertainty associated with TA distance measurements

can use this principle to refine an observed TA command via CeSAR.

Both the initial and maintenance TA are sent in plaintext. The first, which is found in the RAR, is sent before a security key is negotiated and thus must necessarily not be encrypted. The maintenance TA is sent as a MAC CE. Since the CEs are sent as part of the MAC header, which is below the Packet Data Convergence Protocol (PDCP) sublayer, it is also not encrypted. This enables a third party within range to observe this traffic in plaintext. However, if the third party does not observe the initial TA it will be more difficult to effectively use the maintenance TA for ranging as each one is relative to the previous absolute TA maintained by the UE and the network.[11]

4.2 Uncertainty in the Timing Advance

Largely because of the discrete nature of the TA, a single measurement from an eNB will reduce the possible location of the UE to an annulus of fixed width, τ. This annulus, with the eNB as its center, is shown in Figure 4.3. This discrete error is also exacerbated by error associated with the eNB antenna height, multipath propagation, and clock bias [42]. By analyzing the quantization error we can determine the width of the area of uncertainty.

[11]This section was revised from [24].

As stated previously, a TA will change a UE's uplink timing in increments of $16 \times T_s$. The parameter T_s is the LTE basic unit of time and is given by

$$T_s = \frac{1}{15\,000 \times 2048} \text{ seconds} \tag{4.3}$$

where 15 000 corresponds to the subcarrier spacing of 15 kHz and 2048 corresponds to the maximum Fast Fourier Transform (FFT) size [23], [51]. Assuming speed of light propagation, the range of uncertainty τ can then be calculated by

$$\tau = 16 \times \frac{1}{2} \times \frac{c}{15\,000 \times 2048} = 78.125 \text{ meters} \tag{4.4}$$

where c is the speed of light and the extra factor of $1/2$ is included because the eNB must consider the downlink propagation time for the command to reach the UE when issuing a TA.

This line of analysis can also be used to determine the maximum eNB-UE range supportable by LTE. Since the maximum initial TA value is 1282, the formula in (4.4) can be used to determine a maximum supportable distance of approximately 100 km.[12]

4.3 Software Address Space in LTE

Because a multiplicity of users will be simultaneously connected to a given eNB and because each user may be at different distances from the eNB, each UE must be able to determine which TAs are issued to which UEs. To this end, each TA is associated with a destination address in the form of a 16-bit C-RNTI. The C-RNTI is effectively a temporary software address issued by the network to each UE analogous to an Internet Protocol address. The C-RNTI is initially leased to a UE during network access negotiation via the RAR message. Maintenance TAs are associated with a specific C-RNTI via downlink scheduling assignments made on the Physical Downlink Control Channel (PDCCH) found in the L1/L2 control region of each subframe [22]. Because the L1/L2 control region of each subframe needs to be decoded by every UE, it is sent in the clear. Therefore, a third party could use the information in the PDCCH to find the resource on which a transport block for a particular UE is located. The corresponding transport block could then be searched for

[12]This section was revised from [24].

a TA CE. Of particular importance with respect to C-RNTI attribution is that UE network access must be observed in order to initially associate a C-RNTI with a particular UE IMSI as the IMSI is not frequently transmitted unencrypted.[13]

4.4 Timing Adjustment Frequency

The frequency of the maintenance TA is of particular importance as we would like to know how often this information is transmitted and thus how available it is. This frequency is lower bounded by an LTE parameter `timeAlignmentTimer` [54]. This timer is reset each time a TA is received from the eNB. If the timer expires, the radio connection is considered out of synchronization and the UE must renegotiate with the network to restore its uplink time synchronization. Because of this, the TA frequency must ensure a TA is issued within the period of time specified by the `timeAlignmentTimer`. This parameter has configurable finite durations $\{500, 750, 1280, 1920, 2560, 5120, 10240\}$ which is common for all serving cells per UE. The duration corresponds to the maximum number of subframes sent in between TAs. Because subframes are continuous in LTE and because each subframe is stipulated as 1 ms long by the standard, the available durations can also be interpreted as number of milliseconds [51]. Therefore, when configured for finite[14] duration, we can expect a TA to be sent no less frequently than anywhere from every one half second to every ten seconds. In practice, the TA frequency will be more frequent, usually resulting in TAs issued several times per second [22]. During field measurements, we observed TA issuance frequencies at the sub-second level. This frequency of the TA will be sufficient for the purpose of nearly-continuous positioning.[15]

4.5 Heterogeneous Networks

Heterogeneous network deployments were introduced in LTE Release 10 which, among other improvements, allowed for increasing the data capacity of a network through carrier aggregation. Carrier aggregation is a method by which several carriers may be configured to support a single UE. When carrier aggregation is used, a primary cell (PCell) and one or more secondaries (SCell) may be configured to support a single UE. The Radio

[13] This section was revised from [24].

[14] The standard also allows for a configurable infinite duration of `timeAlignmentTimer`.

[15] This section was revised from [24].

Resource Control (RRC) sublayer is responsible for selecting an PCell and then configuring appropriate SCells [54]. Release 11 further provides support for PCells and SCells that are not co-located. In order to maintain uplink synchronization among all serving cells it was necessary to establish the concept of the timing advance group (TAG). Serving cells that are co-located are assigned to the same TAG, thus removing the need for separate TAs for each individual cell. As seen in Figure 4.2, TAGs are associated with TA updates in the two-bit TAG ID field. The size of the TAG ID field indicates the specification is designed to eventually support up to three additional SCells or four total separate channels.[16]

4.6 Timing Advance Positioning during Handovers and with Coordinated Multipoint

In order to facilitate inter-cell mobility, UEs must monitor and evaluate the received signal quality of neighboring cells. The type and frequency of measurements are configurable and are dictated by the network. Measurements normally involve acquisition of the cell PSS and SSS. After this is complete, the UE will have determined the cell-ID and the downlink synchronization giving it access to the cell-specific reference signal. This signal is then used to determine the reference signal received power (RSRP) and/or the reference signal received quality (RSRQ). If the RSRP or RSRQ is larger than a configurable quantity then that cell will be selected for handover. Handovers may occur for various other reasons such as network load management [54].

In the case of a network initiated handover, the UE is notified by the serving eNB via a message that is generated by the target eNB[17]. This message may include mobility information such as the target cell-ID, physical layer parameters, and the new C-RNTI to assist the UE in establishing its new connection. Notably, the handover is asynchronous, meaning the UE will begin the random access procedure with the target eNB which will involve the negotiation of a new initial TA concurrently while still receiving a TA from the source eNB [54].

The presence of two TAs from spatially disparate beacons presents a unique opportunity for gleaning location information. By processing this information at the E-SMLC with

[16]This section was revised from [24].

[17]More specifically, this message is passed as a `RRCConnectionReconfiguration` message [54].

TDoA methods, a hyperbolic annular locus can be described around the source and target eNBs. The advantage of this type of scenario lies in no requirement for the UE to be tightly synchronized with the network effectively removing the error from clock bias. Alternatively, the ToA method may be used which will result in two annuli from the two TAs. The two annuli reduce the target locus to the their area of intersection. Finally, if ciphering is not enabled, the target eNB will issue a new C-RNTI to the UE in the clear allowing a passive listener to map the previous C-RNTI to the new.

Coordinated Multipoint (CoMP), potentially part of Release 11, is a related technique that aims to improve quality of service at cell boundaries by coordinating the reception of a UE signal at multiple eNBs [55]. Uplink timing alignment becomes difficult in such a scenario, as the UE cannot transmit the same signal at different times to ensure each cell receives a time-aligned signal. Solutions to this problem generally involve synchronizing the uplink timing to the nearest serving cell [56] and then selecting other appropriate cells such that the other received signal arrive within the duration of the cyclic prefix [57]. Thus, while it is still an open area of research, the general consensus is for the UE to be uplink synchronized to the closest serving cell [55], [57]. Since CoMP provides no additional location-based information (i.e., the network still only issues one TA) it is not considered further in this study.[18]

4.7 The Empirical Timing Advance

To shed light on the behavior of the TA in the wild, we examine real-world data observed in Maryland and California and shown in Figure 4.4 and Figure 4.5. First we examine the data presented in Figure 4.4, which represents collections where the UE was traveling at a constant rate in a suburban environment such that the distribution of eNB-UE distances during measurement is approximately uniform. From this subset of data, we make two observations.

First, in most cases the variance offered by the TA was relatively small compared to the variances contributed by the measurement error. For example, the average variance among all locations was $\overline{\sigma^2} \approx 3500$ m^2 while the theoretical variance offered by the LTE TA is $\sigma^2_{TA} \approx 500$ m^2.

[18]This section was revised from [24].

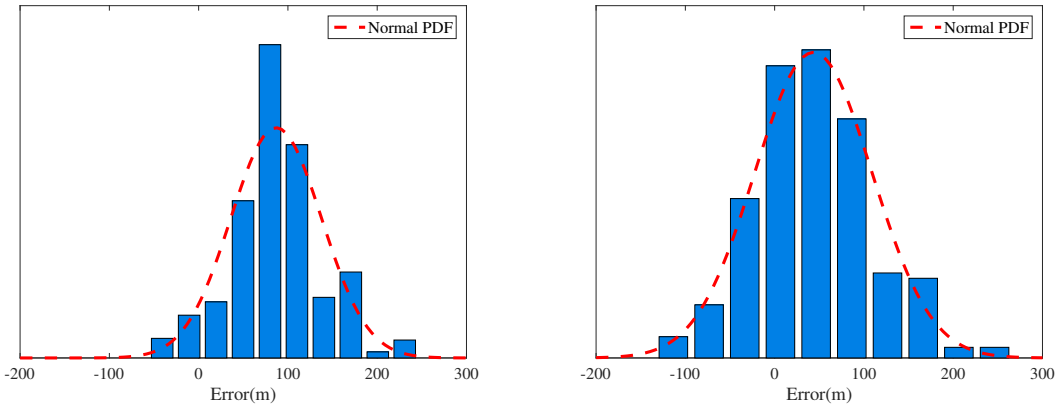
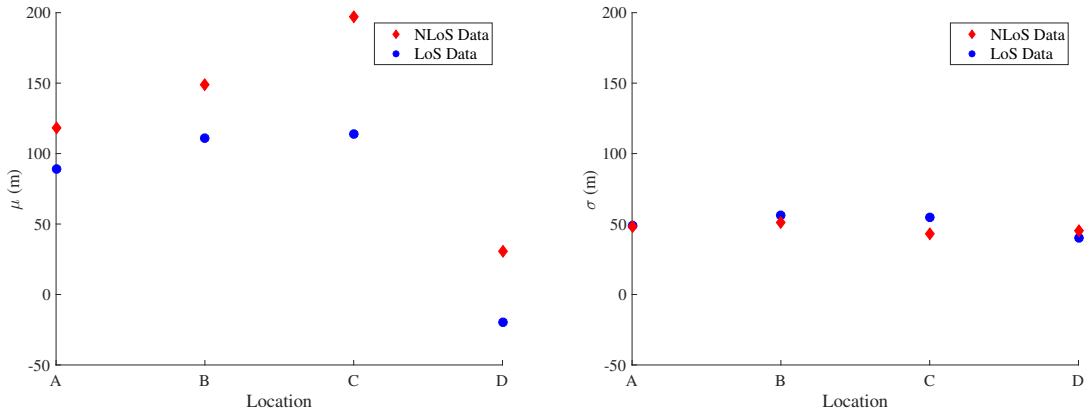


Figure 4.4. Timing advance errors recorded in real-world LTE network deployments in Maryland (a) and California (b). Adapted from [21].

Second, it was previously hypothesized [28] that the underlying error distribution could be modeled as normal. By initial inspection of these data with the normal distribution in Figure 4.4, we find no reason to reject the hypothesis.

Next, we present the results of an experiment conducted at four different locations and designed to elicit the difference in NLoS versus LoS channels. At each of four locations {A,B,C,D}, the distance to a serving eNB was estimated using received TAs. The first- and second-order statistics of the resulting error are presented in Figure 4.5. Each location was characterized as either a dense urban (locations A-C) or suburban environment (location D). Dense urban locations were located in the city center of Baltimore, Maryland, which is largely comprised of tightly-packed skyscrapers. The suburban location was in the outlying area surrounding Baltimore. At each location the distance was fixed (i.e., the UE was stationary) and the TA was recorded for a period of one minute when the serving eNB could be directly seen (LoS). The procedure was then repeated at a nearby location where there was a major obstruction in the line-of-sight to the same serving eNB. Histograms representing the raw error measurements are presented in Appendix A. These histograms can be interpreted as probability mass functions since, with distance constant, the error will be in increments of 78.125 m (c.f. (4.4)).

Referring to Figure 4.5, we observe little difference in standard deviation between LoS



(a) Mean Error (m)

(b) Standard Deviation of Error (m)

Figure 4.5. Data are presented which has been recorded at a fixed distance from eNBs in dense urban and rural environments. Data were recorded when there was a LoS to the eNB and when there was not in the same general location at four different locations {A,B,C,D}. Locations A-C are dense urban environments and location D is a suburban environment. Mean error and standard deviation of error are presented.

or NLoS conditions or dense urban or suburban environments. The measurement error variance can then be considered independent of channel environment which is consistent with the channel model presented in Chapter 2 and with previously reported results [10].

Second, the mean error is highly dependent on channel conditions (i.e., LoS versus NLoS or suburban versus dense urban). As expected, dense urban and NLoS environments resulted in a higher mean error. In all cases the mean error of NLoS measurements was significantly different from the mean error of the LoS measurements at the 5% significance level[19]. Our experiments yielded a $\mu_{\text{NLoS}} - \mu_{\text{LoS}} \in [20\,\text{m}, 80\,\text{m}]$. The difference in urban versus suburban channels was also noticeable. Our experiments showed $\mu_{\text{urban}} - \mu_{\text{suburban}} \in [60\,\text{m}, 220\,\text{m}]$.

Finally, we note that a eNB-specific TA bias is present in each one of the data sets collected. In other words, the mean of all measurements (for constant channel type) will differ. Referring to the measurements presented in Figure 4.5 we see that for LoS environments the mean value has range $\in [-20\,\text{m}, 114\,\text{m}]$. Similarly, for NLoS environments the mean

[19]Statistical difference was established using Student's t-test which requires the underlying data to be normally distributed. Despite the data being discrete, this assumption is further validated through analysis in Chapter 6.

value has range $\in$ [31 m, 197 m]. While it was for these observations that $\mu_{NLoS} - \mu_{LoS} > 0$, the underlying bias is more difficult to predict. This is a value that must be measured and understood *a priori* in order to use the TA to provide an unbiased position estimate. As mentioned in Chapter 3, this quantity is assumed as a given input to the overall scheme.[20]

4.8 The Timing Advance as a Location Privacy Preserving Mechanism

A location privacy preserving mechanism (LPPM) is a paradigm for protecting user location privacy and has two components: obfuscation and anonymization [58]. More specifically, a LPPM is a formal mechanism for modeling the amount of privacy a scheme affords. We thus find it a useful construct in evaluation of the TA since a third party may not have network assistance in obtaining the desired parameters for positioning.

The act of obfuscating a location will add noise to the actual location $\hat{d} = f_1(\mathbf{p})$ thus a third party using obfuscated only data $\langle u_i, \hat{d} \rangle$ will have access to user identities, but the associated location data will be imperfect. The act of anonymizing data will replace the user identity with a pseudonym $\hat{u} = f_2(u_i)$ thus a third party using anonymized only data will have access to exact locations but not identities. A obfuscated and anonymized data set $\langle \hat{u}, \hat{d} \rangle$ will provide a third party access to neither piece of information directly.

Formally, the TA can be modeled as a LPPM. The noise added to the data can be modeled with the function

$$\hat{d}_i = \mathrm{mod}(\parallel \mathbf{p}_i - \mathbf{p}_0 \parallel, \tau) \tag{4.5}$$

assuming an ideal TA model. In other words, the TA obfuscates the actual UE position through a process of spatial quantization. Next, the network anonymizes the UE through assignment of a C-RNTI [22]. As previously discussed, the C-RNTI can be thought of as a software address and is assigned dynamically. Therefore, the C-RNTI mapping $f_{C-RNTI}(\cdot)$ can be thought of as LPPM anonymization.

This LPPM is weak for several reasons. As will later be demonstrated, the quality of the location obfuscation declines rapidly when multiple eNBs are configured. The quality of anonymity provided by $f_{C-RNTI}(\cdot)$ is also in question [59], [60]. We therefore assume

[20]This section was revised from [21].

C-RNTI attribution in this work and focus specifically on de-obfuscation of the UE location $\mathbf{p}_0$.[21]

[21]This section was revised from [28].

CHAPTER 5:
Cellular Synchronization Assisted Refinement

This chapter specifies the details of the Cellular Synchronization Assisted Refinement (CeSAR) algorithm for improving TA-based positioning. Besides details of the algorithm, implementation of the required sensor is also included. CeSAR was first introduced in [24] and is also studied in [21], [28], [29], [61].

This chapter includes adaptations from work submitted for publication or previously published by the author. Specifically, section 5.1 is revised from "On Location Privacy in LTE" by John Roth, Murali Tummala, John McEachen, and James Scrofani which has been submitted for publication [29]. Section 5.3 is revised from "Location Privacy in LTE: A Case Study on Exploiting the Cellular Signaling Plane's Timing Advance" by John Roth, Murali Tummala, John McEachen, and James Scrofani to be published in the proceedings of the 50th Hawaii International Conference on System Sciences in January 2017 [28].

5.1 The Cellular Synchronization Assisted Refinement Algorithm

CeSAR, depicted in Figure 5.1, involves a third party using its knowledge of a UE's transmit timing to refine an area within the initial TA annulus where that UE may be located.

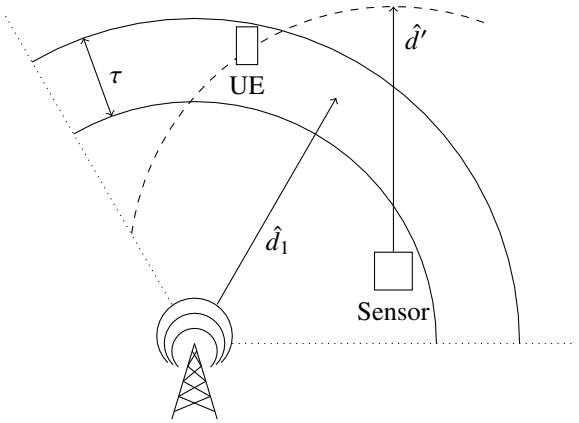


Figure 5.1. A single eNB implementation of the CeSAR algorithm

Algorithm 1 The Cellular Synchronization Assisted Refinement Algorithm. Source: [29].

procedure CeSAR($\mathbf{p}_{eNB}$, $\mathbf{p}_{sensor}$,target C-RNTI)
  function PSS/SSS Sync()
    sensor←eNB downlink frame timing
  end function
  repeat
    x ←observed C-RNTI
  until
  x == target C-RNTI
  $\hat{d}_i \leftarrow$ TA×78.125 m
  $t \leftarrow$ `est_Tx_Time`(TA)
  $t' \leftarrow$ observed uplink burst time
  $\Delta t \leftarrow t' - t$
  $\hat{d}' = \Delta t \cdot c$
  $\hat{\boldsymbol{d}} \leftarrow [\hat{d}_1, \ldots, \hat{d}_N, \hat{d}']^T$
  $\hat{\mathbf{p}} = \arg\min \mathrm{p}(\hat{\boldsymbol{d}}|\mathbf{d})$
end procedure

Generally, the procedure takes advantage of the fact that the TA contains two pieces of information: the distance of the UE to the serving eNB and the UE's uplink transmit time. By exploiting both of these pieces of information, instead of just the eNB-UE distance, a refined position estimate can be made. If a local sensor knows the UE's transmit time t and can record the time t' when the sensor observes the transmission then the distance from the sensor to the UE can be determined by way of UE-sensor propagation delay. In this way, CeSAR applies the principle behind the type 1 TA at the sensor location. As previously stated, this effectively adds another dimension to the system of equations. A necessary requirement to reap this benefit is a sensor in the serving cell/sector of the target UE. In addition to the overall system initialization requirements (cf. Chapter 3), the CeSAR procedure further requires that the position of the sensor be known *a priori*.

Besides improving position accuracy, CeSAR has several strengths [29]:

1. It can be performed completely passively. Therefore, during third party use the sensor cannot be detected from electromagnetic emanations [24].
2. Strategic positioning of the sensor can overcome GDoP [10] caused by eNBs arranged disadvantageously. This is a strength that will be shown in Chapter 8 to improve accuracy significantly [29].

3. The sensor need not be complex. The advent of SDR has put this method within reach of reasonably skilled actors. Furthermore, SDR technology has significantly lowered the monetary cost of entry to this type of exploitation.
4. All of the timing information is sent below the PDCP sublayer, and thus, in the clear [28]. Therefore, there is no need to bypass encryption.

Referring now to Algorithm 1 and Figure 5.1, we give a detailed account of the procedure. First, the sensor listens for the PSS/SSS from a serving eNB (steps 2-4). This is necessary for synchronizing itself to the base station thus giving it the ability to decode cell data. Next, the sensor decodes packets that it receives until it finds the target C-RNTI (steps 5-8). Once a downlink frame being sent to the target UE has been identified (step 8), the associated TA is observed in the MAC CE and converted to the UE-eNB distance $\hat{d}_i$ (step 9). If there are N serving eNBs, this process can be repeated $N-1$ times. Simultaneously, the TA is used to estimate the target UE's uplink transmission time t (step 10). With this information, the sensor can measure the propagation delay Δt from the UE to the sensor and convert that to a UE-sensor distance measurement $\hat{d}'$ (steps 11-13). This additional distance measurement is added to the distance measurements $[\hat{d}_1, \ldots, \hat{d}_N]$ obtained from the N serving eNBs to form the system of equations represented by $\hat{\boldsymbol{d}}$.

Note that steps 10-13 are designed to extract uplink burst timing information from just one of the N serving eNBs. While it is possible to extend CeSAR to repeat these steps across all N eNBs, this will not result in any further information. To see this consider that the extra information gleaned describes a circular locus around the sensor, therefore, additional uplink burst timing information will only re-describe the same circular locus. Thus, attempting to add dimensionality to $\hat{\boldsymbol{d}}$ in this manner will result in dependent equations whose loci will have an infinitude of intersections.

In addition to being nonlinear, the resulting system of equations is inconsistent with high probability due to measurement error induced by the channel (cf. Chapter 2) and spatial quantization associated with the TA, thus, solving this system is non-trivial and the impetus for much of the analysis in Chapter 6. Presently, it is sufficient to treat the nature of the measurement error as following some unspecified probability density $\mathrm{p}(\hat{d}|d)$.

In order to estimate the target UE position, $\hat{\boldsymbol{p}}$, we frame the problem in the maximum-likelihood sense. In other words, for a set of observed distance measurements, $\hat{\boldsymbol{d}}$, the most

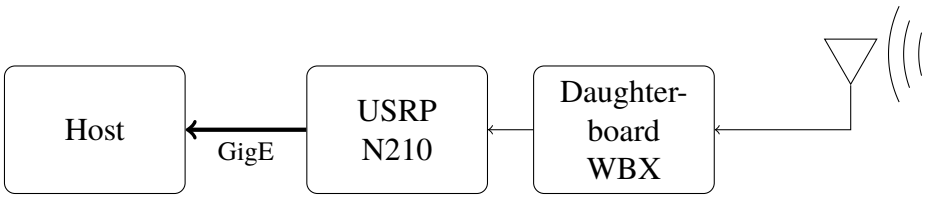


Figure 5.2. The hardware sensor configuration used in this work

likely position estimate is one that satisfies

$$\hat{\mathbf{p}} = \arg\min_{\mathbf{p}} \mathrm{p}(\hat{\boldsymbol{d}}|\mathbf{d}). \tag{5.1}$$

If all measurements follow the same error distribution then we can parameterize the program represented in (5.1) with the distribution $\mathrm{p}(\cdot)$. The claim that $\hat{\mathbf{p}}$ is the *most likely* location of the target UE is heavily dependent on the knowledge of the associated error distributions, thus, characterizing this distribution will be the subject of analysis in Chapter 6.[22]

5.2 Sensor Implementation

As previously discussed, the sensor need not be sophisticated. In fact, modern SDR solutions provide a vehicle by which the sensor can be implemented. At the time of this writing, the necessary RF components for such a SDR solution could be assembled off the shelf for less than $3000. The particular solution implemented by this work is shown in Figure 5.2.

The RF front end is a universal software radio peripheral (USRP) N210 manufactured by Ettus Research. The processing speed is high enough in this peripheral such that the maximum sample rate is limited by the Gigabit Ethernet connection to the host machine which is nominally 20-25 MSps. The RF daughterboard utilized is the WBX board also manufactured by Ettus Research. This daughterboard is capable of modulating/demodulating baseband signals frequencies in the range of 50-2200 MHz which sufficiently covers the cellular spectrum.

[22]This section was revised from [29].

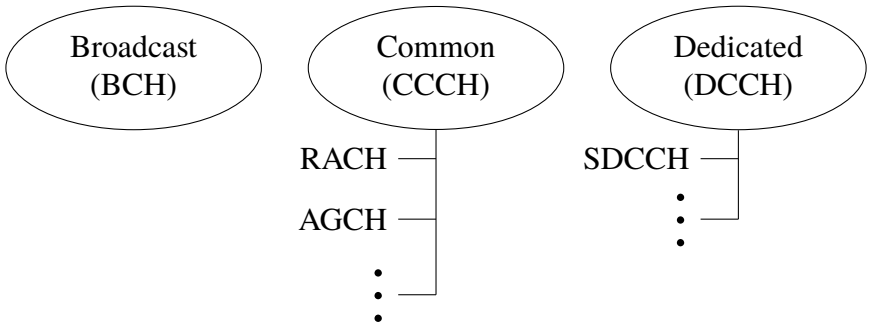


Figure 5.3. An overview of the salient logical signaling channel organization in GSM

5.3 Observability of Uplink Frames

Here we highlight step 11 of the CeSAR algorithm which requires that a sensor is able to observe an uplink burst from a specific UE. Because LTE uses an OFDMA access scheme [22], the sensor would need to know what resource element(s) were assigned by the network to that UE. Learning this information without direct access to an eNB is non-trivial, however, possible. This possibility, which is the focus of this section, marks a significant shift in the confidentiality architecture of LTE. In this section, we contrast the signaling plane confidentiality of LTE with that of GSM to first highlight this shift. Additionally, the contrast demonstrates that, while it is not possible to decode the UE uplink burst, it is possible to know in what time-frequency resource it will be sent.

We begin by first presenting the salient aspects of the GSM signaling plane. GSM defines a series of logical channels used in both the downlink and uplink. They are broken into two categories of traffic and signaling planes, the latter of which is shown in Figure 5.3. In the signaling plane are three groups of channels: the broadcast (BCH), common control (CCCH), and dedicated control channel groupings (DCCH).

Of specific interest are the CCCH and DCCH groupings. Among other things, the CCCH is responsible for the random access procedure via the random access channel (RACH) and the access grant channel (AGCH) [62], [63]. Of note, no channels in the CCCH group are encrypted as they contain information relevant to multiple users [64].

Consider a UE with information to transmit to the network and without a current valid scheduling grant. The UE first needs to request assignment of a Standalone Dedicated

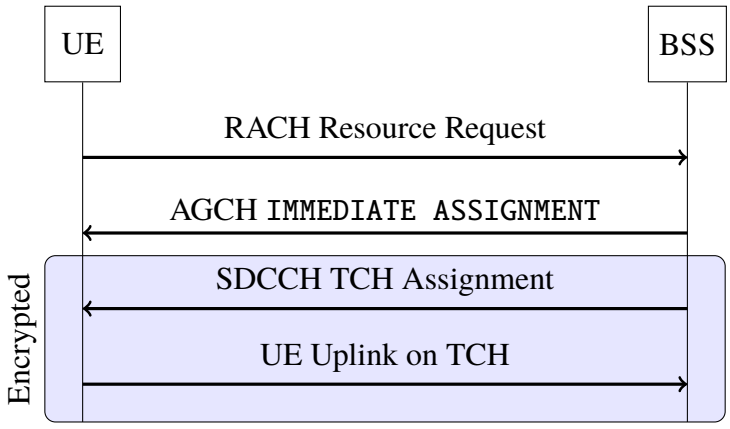


Figure 5.4. The radio resource allocation procedure for a GSM connected UE with network traffic

Control Channel (SDCCH) via the RACH [63]. The base station controller (BSC) will respond with an `IMMEDIATE ASSIGNMENT` message via the AGCH assigning a specific SDCCH to the requesting UE. Once the SDCCH is assigned encryption will begin. Finally, an encrypted `ASSIGNMENT COMMAND` gives the parameters of the traffic channel (TCH) to the UE [62]. Because this last step is performed after encryption begins, the confidentiality of the uplink channel signaling is effectively preserved in GSM. This process[23] is presented graphically in Figure 5.4.

Of particular interest is that encryption in the GSM air interface is performed at a very low level immediately preceding modulation (in logical channels that support encryption) [62]. This strengthens the confidentiality of signaling traffic.

Similar to GSM, LTE also specifies a series of logical channels albeit organized differently than in GSM. LTE has a more flat channel architecture so a hierarchy is not presented. Rather only specific channels are selected for discussion. They are broken into the downlink and uplink subgroups of which the former is of particular interest. In this group there exists a DCCH similar to that of GSM, however, different from GSM the LTE DCCH is a bearer of mainly the Radio Resource Control (RRC) layer information. Also different from GSM, LTE specifies certain physical channels onto which no logical channel will map. Of interest to this work is the Physical Downlink Control Channel (PDCCH) and the Physical Uplink

[23]Only an overview of the major steps in the process are presented for clarity. Furthermore, the base transceiver station (BTS) and base station controller (BSC) are grouped into one entity, the base station subsystem (BSS).

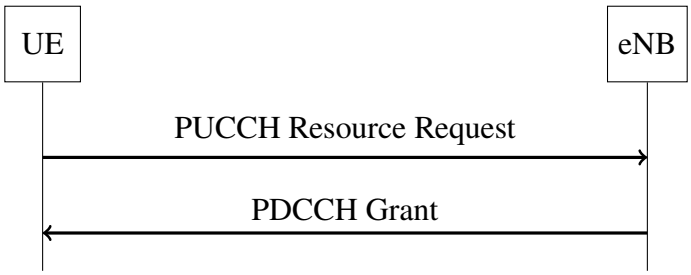


Figure 5.5. The radio resource allocation procedure for an LTE connected UE with network traffic is presented. Only an overview of the major steps in the process is presented for clarity.

Control Channel (PUCCH).

In LTE, scheduling is the responsibility of the MAC layer and is done dynamically on a frame-by-frame (i.e., 1 ms) basis [22][24]. Therefore, unlike GSM, LTE does not assign dedicated control channels (i.e., the GSM SDCCH). Instead, the information pertaining to uplink scheduling is found in the PDCCH broadcast in the L1/L2 control region of each downlink frame [22].

Consider a UE with information to transmit to the network and without a current valid scheduling grant. The UE will first utilize the uplink L1/L2 control region to indicate to the eNB that it requires uplink resources. As previously discussed, the eNB's scheduling decisions are issued via the PDCCH in the L1/L2 control region. Each scheduling grant is appended with a cyclic redundancy check (CRC) which is calculated with the intended recipient's radio network temporary identifier (RNTI). Therefore all grants sent via the PDCCH are checked by each UE with their allocated RNTIs. Grants that do not check are discarded as either not intended for the UE or invalid [22]. The PDCCH is continuously monitored by each connected UE to update its uplink grant allocation as it is changed dynamically. This process is presented graphically in Figure 5.5.

Next, a large functional change in LTE, relative to GSM, is highlighted: *the responsibility for encryption is held exclusively in the PDCP sublayer*. Therefore, nothing in the lower layers (i.e., the Radio Link Control (RLC) and MAC layers) is ciphered [47]. A consequence of this architectural shift is that a significant amount of signaling is sent in the clear. The

[24]It should be noted that the network can also optionally choose to implement semi-persistent, vice dynamic, scheduling.

requirement for transparent signaling is also built into the uplink scheduling scheme (cf. Figure 5.5) which would not work if ciphering was implemented at the same low level it is in GSM. Therefore, with this signaling plane confidentiality, the target RNTI is only needed to decode that UE's unencrypted uplink resource grants.[25]

[25]This section was revised from [28].

CHAPTER 6:
Theory of Random Variable Quantization

In this chapter, following [65], we provide an account of the theory of quantization of a RV in general terms. To provide an impetus for the subsequent discussion, we first introduce fundamental and relevant concepts such as the CRLB and GDoP. We then derive the conditions necessary to satisfy a lower bound on positioning. This chapter provides the theoretical foundation and justification for a method of maximum-likelihood estimation developed in the subsequent chapter and follows directly from work previously published by the authors [21], [29]. Specifically, Sections 6.1 and 6.2 are revised from "Maximum Likelihood Geolocation in LTE Cellular Networks Using the Timing Advance Parameter" by John Roth, Murali Tummala, John McEachen, James Scrofani, and Robert DeGabriele to be published in the proceedings of the 10th International Conference on Signal Processing and Communication Systems in December 2016 [21]. Sections 6.4- 6.9 are revised from "On Location Privacy in LTE" by John Roth, Murali Tummala, John McEachen, and James Scrofani which is submitted for publication [29].

6.1 The Cramér-Rao Lower Bound in Time of Arrival Positioning

The CRLB is a well-known lower bound on the mean square error (MSE) or root mean square error (RMSE) of an unbiased estimator [7], [10], [48]. In this work, we use the RMSE in order to provide results that are easier to understand in terms of positioning accuracy. Given the unbiased estimate $\hat{\mathbf{p}}$, the CRLB is formally expressed as

$$\sqrt{\mathrm{E}\{(\mathbf{p}_0 - \hat{\mathbf{p}})^2\}} \geq \mathrm{CRLB}. \tag{6.1}$$

In matrix form, $\mathrm{CRLB} = \mathrm{Tr}(\sqrt{\mathbf{I}^{-1}})$ where $\mathrm{Tr}(\cdot)$ is the trace function and $\mathbf{I}$ is the Fisher information matrix (FIM) developed for the ToA application as [10]

$$\mathbf{I}_{\{i,j\}} = -\mathrm{E}\left\{\frac{\partial^2 \log \mathrm{p}(\hat{\boldsymbol{d}}|\mathbf{d})}{\partial \mathbf{p}_{\{i\}} \partial \mathbf{p}_{\{j\}}}\right\} \tag{6.2}$$

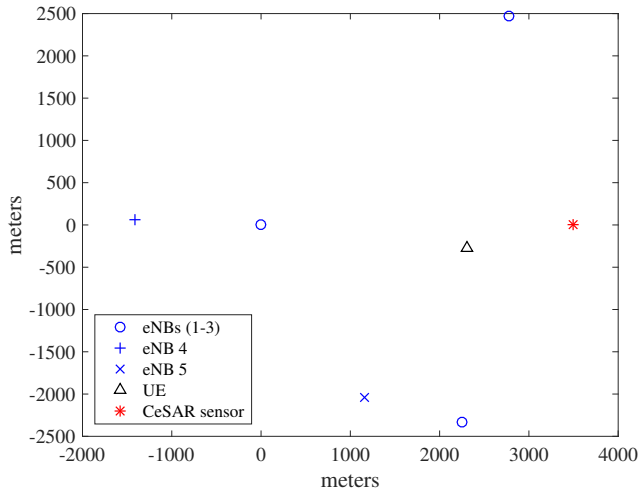


Figure 6.1. The layout of an actual cellular network deployment located in Annapolis, Maryland. Source: [21].

where the subscript(s) in brackets represent the matrix or vector index. The proof of this relationship for a general unbiased estimator is provided in Appendix B. When the probability distribution function (PDF) is normal and $\sigma_i = \sigma$, $\forall i$, it can be shown that [31]

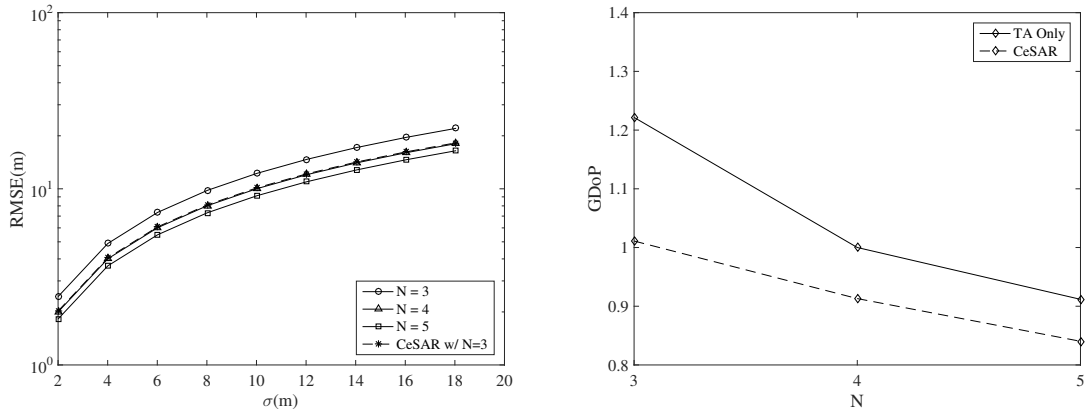
$$\mathbf{I} = \frac{1}{\sigma^2} \begin{bmatrix} \sum_{i=1}^{N} \frac{(x-x_i)^2}{d_i^2} & \sum_{i=1}^{N} \frac{(x-x_i)(y-y_i)}{d_i^2} \\ \sum_{i=1}^{N} \frac{(x-x_i)(y-y_i)}{d_i^2} & \sum_{i=1}^{N} \frac{(y-y_i)^2}{d_i^2} \end{bmatrix}. \tag{6.3}$$

A proof of the relationship presented in (6.3) is given in Appendix C. In general, the expectation in (6.2), taken with respect to $\mathbf{p}$, may not have a closed-form solution. In this case, it is necessary to resort to numerical integration techniques.

When NLoS conditions are present, it has been shown that the CRLB can be attained when the eNB(s) with NLoS channel conditions are discarded and only those remaining with LoS conditions are used for positioning [66]. This requires the ability to identify and discard those measurements [31].

In order to show typical values of the CRLB, an actual network deployment in Annapolis, Maryland, shown in Figure 6.1, was evaluated[26]. The fourth and fifth nodes are added

[26]Latitude and longitude have been converted to the Cartesian coordinate system where the axes units are given in meters.



(a) (b)

Figure 6.2. The curves in the left pane show the CRLB as parameterized by the noise level σ and the number of eNBs N. The GDoP is also shown in the right pane to demonstrate the favorability of the eNB geometry as nodes 4 and 5 are added. Source: [21].

successively to show how positioning changes as more nodes become available. The theoretical lower bound on the accuracy of an unbiased estimator for this geometry is then shown in Figure 6.2 along with the corresponding trends in GDoP. In the left pane, the abscissa represents the error in distance estimation given $\sigma_i = \sigma$, $\forall i$. The values are chosen as they are common error variances in ToA positioning [31]. The ordinate represents the minimum localization RMSE possible in meters. In the left pane, the abscissa represents the number of eNBs N and the ordinate shows the GDoP value for the given N.

The CRLB can then be said to be a function of several parameters:

1. The shape of the probability density. The more peaked the shape (i.e., kurtosis), the lower the CRLB (cf. (6.2)).
2. The variance of the error associated with the parameter to be estimated. The lower the variance, the lower the CRLB (cf. Figure 6.2 and (6.3)).
3. The number of available eNBs. In general, the more eNBs available, the lower the CRLB (cf. Figure 6.2 and (6.3)).
4. The geometry of the eNBs. It can be seen in (6.3) that, for the case of a normal density, the geometry is completely defined by the angle from the UE to the eNB(s)

and the distance is mathematically irrelevant[27].

The sole dependence of the CRLB on the associated angles in the geometry and not the distance can be seen from the following identities

$$\begin{aligned} \cos(\theta_i) &= \tfrac{(x-x_i)}{d_i} \\ \sin(\theta_i) &= \tfrac{(y-y_i)}{d_i} \end{aligned} \tag{6.4}$$

where θ is the angle subtending the i^{th} eNB and the UE. Substituting these identities into (6.3) we have

$$\mathbf{I} = \frac{1}{\sigma^2}\begin{bmatrix} \sum_{i=1}^{N} cos^2(\theta_i) & \sum_{i=1}^{N} cos(\theta_i)sin(\theta_i) \\ \sum_{i=1}^{N} cos(\theta_i)sin(\theta_i) & \sum_{i=1}^{N} sin^2(\theta_i) \end{bmatrix}. \tag{6.5}$$

From (6.5) it is easy to see how the CRLB is not dependent on distance.[28]

6.2 Geometric Dilution of Precision in Time of Arrival Positioning

It was stated in the previous section and expressed in (6.3) that the CRLB is a function of the eNB geometry. The effect of the geometry can be isolated from the effect of the measurement noise by dividing out the measurement error to yield the GDoP given as [10]

$$\text{GDoP} = \frac{\sqrt{\text{Tr}(\mathbf{I}^{-1})}}{\sigma}. \tag{6.6}$$

GDoP can generally be interpreted as the factor by which the standard deviation of the position estimate is related to the standard deviation of the distance measurement

$$\sqrt{\text{E}\left\{(\mathbf{p}_0 - \hat{\mathbf{p}})^2\right\}} = \text{GDoP} \times \sqrt{\text{E}\left\{(d - \hat{d})^2\right\}}. \tag{6.7}$$

As a rule of thumb, it has been previously reported that GDoP values of less than three are favorable where values greater than six are not [10]. Additionally, values of less than one are

[27] It has been previously reported that the standard deviation of the distance measurement is distance dependent [67]. Therefore, although d_i does not affect the CRLB directly the variance may actually be a function of the distance (i.e., $\sigma_i(d_i)$).

[28] This section is revised from [21].

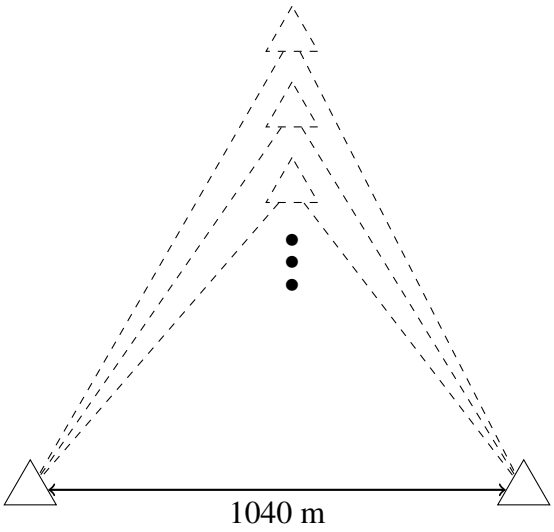


Figure 6.3. The experimental setup of the GDoP investigation

possible and imply that the position estimate will have a smaller standard deviation than the individual distance estimates, thus a geometric concentration of precision is experienced.

In order to investigate the geometric effect of eNBs on positioning we again turn to Figure 6.2. Here the right pane shows how the geometric state improves as each eNB is added with and without CeSAR. Without CeSAR, after the fifth eNB is made available the GDoP is actually less than one where the aforementioned implication about geometric concentration of precision applies.

In traditional cellular networks one is limited to the GDoP offered by the existing geometry. However, one advantage of CeSAR is that the location of the CeSAR sensor can be chosen to minimize GDoP. The geometric advantage of CeSAR is again shown in the right pane of Figure 6.2. With CeSAR, the GDoP starts at one when $N = 3$ and continues to improve as N increases.

To generalize the idea of GDoP beyond this specific use case we propose a notional model of three eNBs arranged as an isosceles triangle as in Figure 6.3. The eNBs are all approximately one kilometer apart. An area of one square kilometer, centered on the center of mass of the triangle, is chosen as an area reasonably served by all three eNBs. The geometry of the eNBs is systematically changed by lowering the base angle of the isosceles triangle (keeping the base distance constant). The GDoP is then sampled uniformly throughout the serving

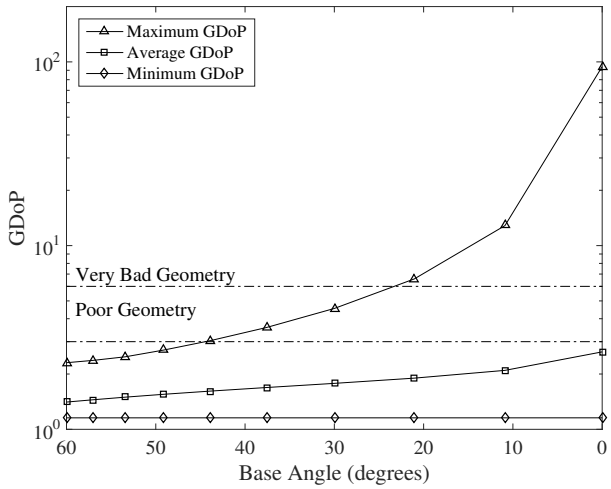
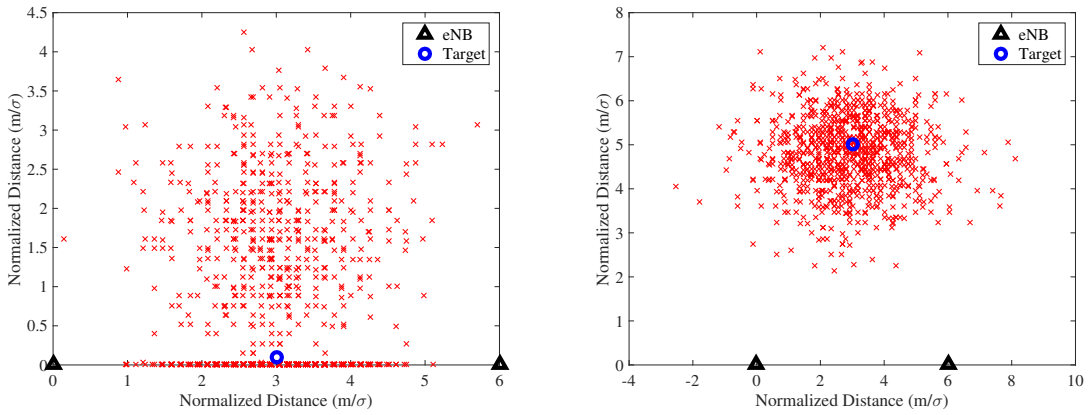


Figure 6.4. The maximum, minimum, and mean GDoP in a serving area of a collection of three serving eNBs is presented here. The eNBs are arranged in an isosceles triangle with the base edge approximately one kilometer long and with the base angle specified by the abscissa. Source: [21].

area and the results recorded in Figure 6.4. The regions of GDoP noted by [10] as having suboptimal geometries for positioning, according to the aforementioned rule of thumb, are shown in the figure. The maximum GDoP within the region quickly exceeds acceptable limits while the mean and minimum remain within acceptable limits throughout. This trend across statistics suggests that the more collinear eNBs are in the geometry, the worse the environment for positioning. We note that this study is conservative as the maximum values of GDoP remain on-axis with the triangle base and outside of the convex hull of the triangle which is not well represented by the serving area.

These results suggest that, on average, the geometry of eNBs should not be unfavorable. While GDoP will always affect the accuracy of the position estimate, even with very severe collinear eNB geometry (such as that seen frequently in main thoroughfares like major highways), harsh GDoP effects may not be common. An interesting corollary is that because GDoP is only a function of the angles between the UE and eNBs (cf. (6.5)) the density of eNBs will not have an effect on the positioning accuracy. Therefore we should not expect that the recent move towards cell densification [68], as a means to increasing data throughput, will improve positioning performance purely vis-à-vis denser infrastructure



(a) Pathological Geometry (b) Normal Geometry

Figure 6.5. Geometric pathology in a two eNB positioning scenario

geometry.[29]

6.3 Pathological Geometries

The CRLB is only a meaningful lower bound if the estimate is unbiased [48]. However, the infrastructure may be physically organized such that an unbiased estimate is not possible. We call this situation a *pathological geometry*. To understand this phenomenon, consider the positioning scenarios shown in Figure 6.5. In both figure panes a Monte Carlo study is conducted where there are two serving eNBs ($N = 2$) from which a target will be located. The distance estimate made from each eNB is corrupted by a normal error source. The axes are given in distance normalized by the standard deviation where $\sigma_1 = \sigma_2$. Since, in a two eNB scenario, it is equally as likely that the UE is on either side of the abscissa we restrict the solution space to points which lie above the x-axis. In the left pane, the UE to be located is almost directly in between the two eNBs. In the right pane, the UE to be located is offset by 5σ. By inspection of the resulting probability clouds, it is not hard to see that the geometry in the left pane is biased while the geometry in the right pane is not.

This pathology arises from the fact that the CRLB does not take symmetry into account which naturally arises in a two eNB scenario (i.e., it is equally likely that the position estimate is above or below the x-axis for a given set of distance estimates). The symmetry

[29]This section is revised from [21].

is described in this scenario by the line $y = 0$, which we term the *symmetry directrix*. Symmetry of this sort can be dealt with by artificially restricting the solution space, as we have done in Figure 6.5. Not doing this dramatically increases the resulting error since if the position estimate on the wrong side of the directrix is chosen the error will be much larger. Therefore, regardless of whether the solution space is artificially restricted or not, the estimate will be biased. To see this, consider the pathological geometry in the left pane of Figure 6.5 and note that a significant number of position estimates lie approximately on the x-axis. This arises from the scenario where the sum of the distance estimates from the eNBs is less than the distance between the eNBs. Put another way, if the distance estimates were represented as circles centered on their respective eNBs, they would not intersect. It is clear that in this scenario the *most likely* position estimate will lie somewhere on the line connecting the two eNBs. In fact, for this scenario, this will happen approximately one-half of the time and is a significant source of bias. In contrast, when the target moves far enough away from the eNBs this bias disappears since the distance estimate circles will intersect the vast majority of the time. In this case the probability cloud that is generated looks as we would expect one to look that was generated from normal error. Alternatively, if a third eNB is included, the bias will also disappear since the third eNB will help adjudicate the position estimate in the direction orthogonal to the symmetry directrix.

Bias will be introduced anytime a position estimate is found without sufficient information in each of the orthogonal bases for the coordinate system in use (seen in the left pane of Figure 6.5). For measurements with normally distributed error and two eNBs, this means the UE should be at least 3σ away from the directrix. The rule of thumb to avoid bias is less straightforward when $N > 2$ where numerical means can be used to estimate bias.

6.4 The Probability Density of a Quantized Random Variable

Quantization is sometimes regarded as a non-linear operation making analysis of the associated operations difficult. Here we review the work presented in [65] and highlight that quantization can be shown to be a linear injective operation in the RV signal space. This realization will justify use of the latent continuous distribution in a MLE.

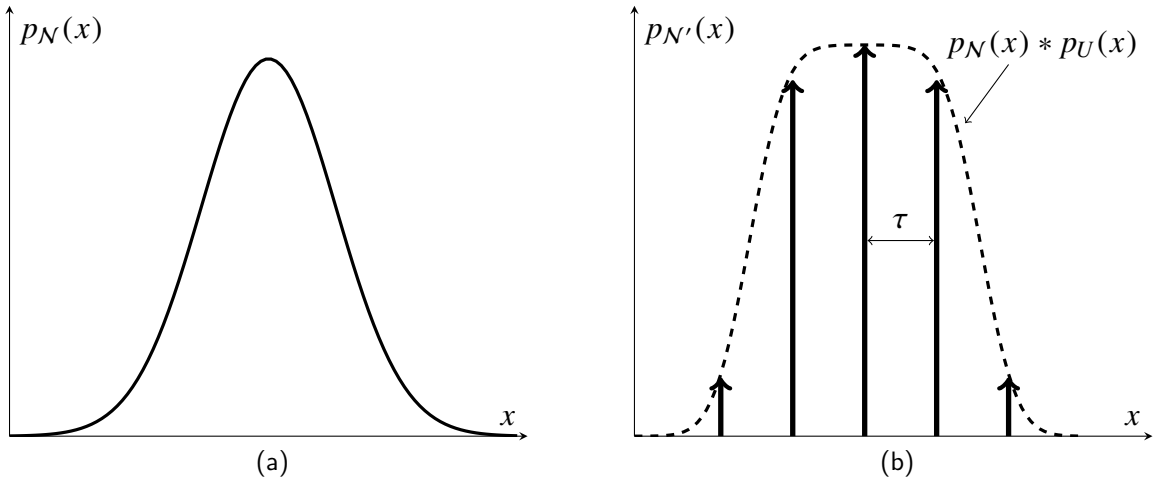


Figure 6.6. The mapping of $Q : \mathcal{N} \longmapsto \mathcal{N}'$. Adapted from [29].

First, consider a latent RV $\mathcal{N}$ which, has the specific probability density

$$p_{\mathcal{N}}(x) = \frac{1}{\sqrt{2\pi}\sigma} e^{\frac{-x^2}{2\sigma^2}} \tag{6.8}$$

and cumulative distribution function

$$F_{\mathcal{N}}(x) = \Phi\left(\frac{x}{\sigma}\right) \tag{6.9}$$

such that $\mathcal{N}$ has zero mean and some variance σ. For convenience, and due to the assumption that $\sigma_i = \sigma \; \forall i$, we hereafter use only $\Phi(x)$ to represent the cumulative density of $\mathcal{N}$. We define the specific distribution of $\mathcal{N}$ to simplify the discussion of quantization on variance (cf., Figure 6.6) although the analysis presented is applicable to other distributions. We will later show this choice of a normal distribution is appropriate for TA-based positioning.

Next, consider a quantization function Q such that $Q : \mathcal{N} \to \mathcal{N}'$ and the density of $\mathcal{N}'$ is given as

$$p_{\mathcal{N}'}(x) = \sum_n \alpha_n \delta(x - n\tau). \tag{6.10}$$

Here we make use of the shorthand $\sum_n$ to represent the sum over all $n \in \mathbb{Z}$, $\delta(\cdot)$ to represent the Dirac delta function, and α to represent some appropriate scaling parameter. The relation in (6.10) can be regarded as a quantized version of $\mathcal{N}$ with bins evenly spaced by τ.

It is well-known that the quantization operation contributes to the overall noise of the resulting signal. This is represented by the convolution $p_{\mathcal{N}}(x)$ with a uniform distribution $p_U(x)$ with support $\in [-\tau/2, \tau/2]$. As a first step in defining $\mathcal{Q}$, consider the result of this convolution which is presented in detail in Appendix D

$$p_{\mathcal{N}}(x) * p_U(x) = \frac{1}{\tau}\left[\Phi\left(x + \tau/2\right) - \Phi\left(x - \tau/2\right)\right] \tag{6.11}$$

where $\Phi(x - \psi)$ is the cumulative density of $p_{\mathcal{N}}(x)$ shifted by some amount ψ. The second and final step taken in defining $\mathcal{Q}$ is a multiplication of (6.11) with an impulsion train (Dirac comb) scaled by τ, $\text{Ш}_\tau(x)$, with periodicity τ. This process is presented graphically in Figure 6.6.

To verify that (6.10) follows, observe that

$$\begin{aligned}\left(\sum_n \tau\delta(x - n\tau)\right)\frac{1}{\tau}\left[\Phi(x + \tau/2) - \Phi(x - \tau/2)\right] = \\ \sum_n \delta(x - n\tau)\left[\Phi(n\tau + \tau/2) - \Phi(n\tau - \tau/2)\right].\end{aligned} \tag{6.12}$$

Next, let

$$\alpha_n = \left[\Phi(n\tau + \tau/2) - \Phi(n\tau - \tau/2)\right]. \tag{6.13}$$

Finally, by substituting (6.13) into (6.12) we arrive at (6.10).

To see the equivalency of $\mathcal{Q}$ to quantization consider (6.11) as the difference of two scaled cumulative densities (c.f., Figure 6.6). The product of that density with a Dirac delta results in

$$\begin{aligned}\tau\delta(x - x_1)\left(p_{\mathcal{N}}(x) * p_U(x)\right) =& \delta(x - x_1)[\Phi(x_1 + \tau/2) - \Phi(x_1 - \tau/2)] \\ =& \delta(x - x_1)\int_{x_1-\tau/2}^{x_1+\tau/2} p_{\mathcal{N}}(x)\,dx \\ =& \alpha_{x_1/\tau}\delta(x - x_1)\end{aligned} \tag{6.14}$$

where the Dirac delta represents a bin centered on x_1. The result of the product, given in (6.14), is exactly the quantization operation, shown in Figure 6.7, a direct result of the definition of a cumulative distribution function.

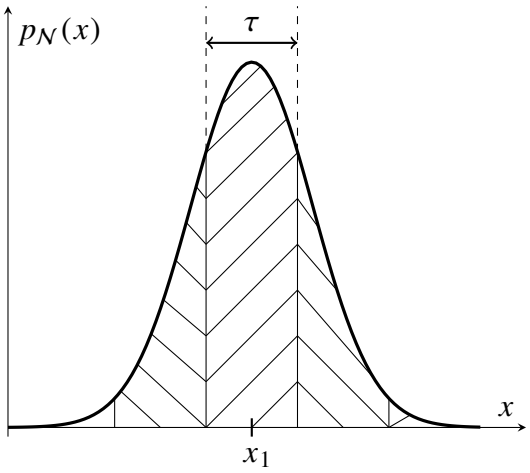


Figure 6.7. The quantization of a normal RV with bin size τ and bin centers $x_1 + n\tau$ is presented here. Adapted from [65].

Note that all steps taken in $\mathcal{Q}$ are linear and thus also commute. Therefore, while the operation is indeed non-linear in the observation space (i.e., the result of a quantized observation cannot be undone), the operation is linear in signal space. This will be the subject of further discussion in a subsequent section.[30]

6.5 The Characteristic Function of Quantized Random Variable

Consider $p_{\mathcal{N}}(x) \overset{\mathcal{F}}{\longleftrightarrow} P_{\mathcal{N}}(\phi)$ which are related via the Fourier transform and define $P_{\mathcal{N}}(\phi)$ as the characteristic function (CF) of $p_{\mathcal{N}}(x)$. The Fourier equivalent steps that define the mapping of the CFs under $\mathcal{Q}$ is shown graphically in Figure 6.8 and given precisely by $\text{Ш}_{2\pi/\tau}(\phi) * P_{\mathcal{N}}(\phi) \cdot P_U(\phi)$ which yields

$$P_{\mathcal{N}'}(\phi) = \sum_n A_n(\phi - 2\pi n/\tau). \tag{6.15}$$

Here $A(\phi)$ is the result of the product of CFs $P_{\mathcal{N}}(\phi)$ and $P_U(\phi)$ explicitly given by

$$P_{\mathcal{N}}(\phi) \cdot P_U(\phi) = e^{\frac{-(\phi\sigma)^2}{2}} \operatorname{sinc}\left(\frac{\phi\tau}{2}\right) \tag{6.16}$$

[30]This section is revised from [29].

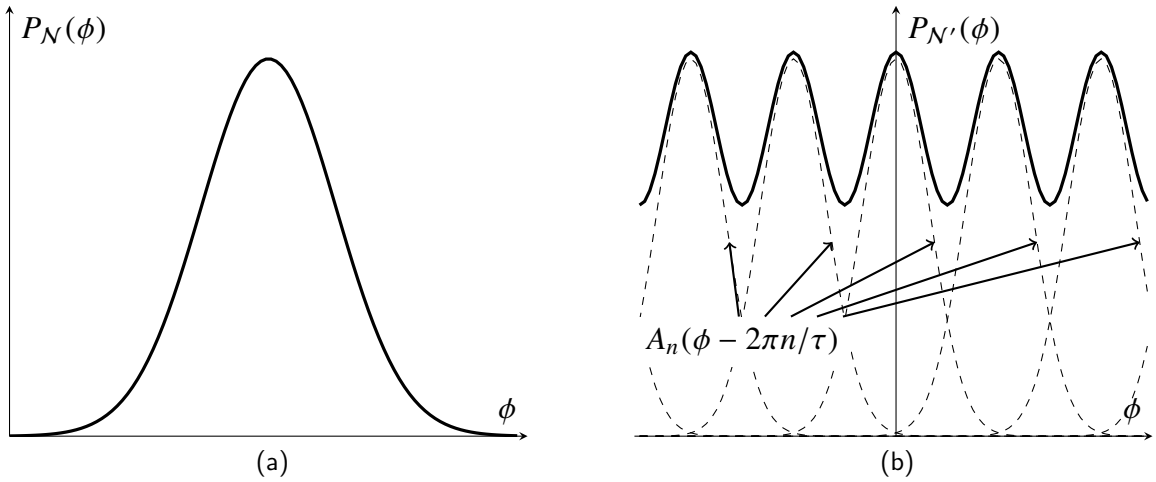


Figure 6.8. The mapping of $Q : \check{\mathcal{N}} \longmapsto \check{\mathcal{N}}'$

where the product itself is trivial and the derivation of the exact CFs for $P_{\mathcal{N}}(\phi)$ and $P_U(\phi)$, given $\mathcal{N}$ is normal, can be found in Appendix E. Finally, we arrive at $P_{\mathcal{N}}(\phi)$ by performing the convolution

$$\text{Ш}_{2\pi/\tau}(\phi) * P_{\mathcal{N}}(\phi) \cdot P_U(\phi) = \sum_n e^{\frac{-((\phi-2\pi n/\tau)\sigma)^2}{2}} \operatorname{sinc}\left(\frac{(\phi - 2\pi n/\tau)\tau}{2}\right). \tag{6.17}$$

By comparing (6.17) to (6.15) we can see that

$$A(\phi) = e^{\frac{-(\phi\sigma)^2}{2}} \operatorname{sinc}\left(\frac{\phi\tau}{2}\right) \tag{6.18}$$

and the separation of $A_n(\phi)$ is inversely proportional to τ. To graphically show the effect of Q in the Fourier domain, the $A_n(\phi)$ are shown in Figure 6.8 with dashed lines while their sum is shown with a boldface line. Also, the quantization operation in the Fourier domain is completely defined by linear operations, thus fully injective in the RV parameter space. Stated another way, given a quantized probability density function one is able to recover the latent probability density function[31] by reversing the above steps. The fact that quantization is injective in the RV parameter space in both domains is an important point that will be used to justify later statistical claims.[32]

[31]We note that certain conditions must be met in order for this to be true and are discussed later in this chapter.

[32]This section is revised from [29].

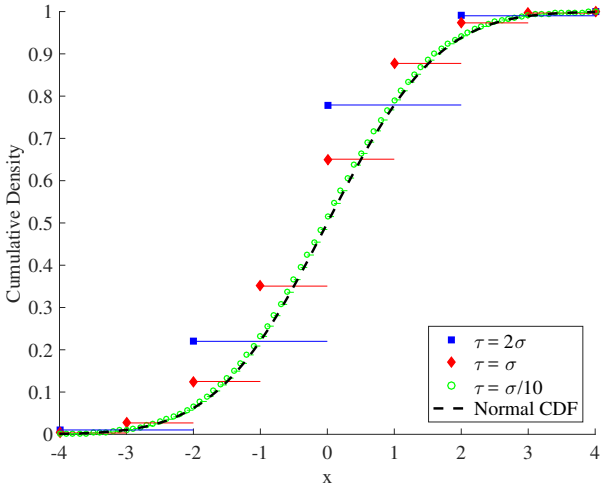


Figure 6.9. The cumulative density function of $p'_{\mathcal{N}}(x)$ as $\tau \to 0$

6.6 The Effect of Quantization Bin Size

Next we vary τ to examine the effect of the bin size on $p_{\mathcal{N}'}(x)$ and $P_{\mathcal{N}'}(\phi)$. We will later expand on these observations to explain the effect of τ on the variance of $\mathcal{N}'$.

6.6.1 The Effect of Quantization Bin Size as $\tau \to 0$

To understand the effect of a decreasing τ on (6.10) and (6.15) let $\tau \to 0$ and let

$$F_{\mathcal{N}'}(x) = \Pr[\mathcal{N}' \leq x] \tag{6.19}$$

so that $F_{\mathcal{N}'}(x)$ is the cumulative distribution function of $\mathcal{N}'$. Using (6.10) and (6.13) we can define the cumulative distribution function explicitly as

$$\begin{aligned} F_{\mathcal{N}'}(x) &= \sum_{n=-\infty}^{\lfloor x \rfloor_\tau} \alpha_n \\ &= \sum_{n=-\infty}^{\lfloor x \rfloor_\tau} [\Phi(n\tau + \tau/2) - \Phi(n\tau - \tau/2)] \\ &= \Phi\left(\lfloor x \rfloor_\tau\right) \end{aligned} \tag{6.20}$$

where $\lfloor \cdot \rfloor_\tau$ is the floor operator taken with respect to τ. Next observe that

$$\lim_{\tau \to 0} \Phi\left(\lfloor x \rfloor_\tau\right) = \Phi(x) \tag{6.21}$$

therefore the cumulative density of $\mathcal{N}' \to \mathcal{N}$ as $\tau \to 0$ since

$$\lim_{\tau \to 0} \lfloor x \rfloor_\tau = x. \tag{6.22}$$

This convergence in $\tau \to 0$ of $F_{\mathcal{N}'}(x) \to F_{\mathcal{N}}(x)$ is shown graphically in Figure 6.9. It follows then that

$$\lim_{\tau \to 0} p_{\mathcal{N}'}(x) = p_{\mathcal{N}}(x). \tag{6.23}$$

From this relationship it is a trivial step to see that

$$\lim_{\tau \to 0} P_{\mathcal{N}'}(\phi) = P_{\mathcal{N}}(\phi) \tag{6.24}$$

since $p_{\mathcal{N}}(x) \overset{\mathcal{F}}{\longleftrightarrow} P_{\mathcal{N}}(\phi)$. To verify, consider $P_{\mathcal{N}'}(\phi)$ and note that as $\tau \to 0$ the separation between $A_n(\phi)$ increases to ∞. Therefore, we can say that

$$\lim_{\tau \to 0} P_{\mathcal{N}'}(\phi) = A_0(\phi) \tag{6.25}$$

and note that $A_0(\phi) = P_{\mathcal{N}}(\phi)$ which verifies the relationship in (6.24).

Another intuitive way of verifying this relationship is to note that as $\tau \to 0$ we are no longer quantizing the latent RV. This view is consistent with (6.23) and (6.24).

6.6.2 The Effect of Quantization Bin Size as $\tau \to \infty$

To illuminate the effect of an increasing τ on (6.10) and (6.15) consider the case when $\tau \to \infty$. It can be seen that

$$\lim_{\tau \to \infty} p_{\mathcal{N}'}(x) = \delta(x) \tag{6.26}$$

since as $\tau \to \infty$, $a_0 \to 1$ and $a_n \to 0$, $\forall n \neq 0$. Note that as $\tau \to \infty$ the center bin extends to cover all of $\mathbb{R}^1$ and thus the output of the quantizer is deterministic. To see this, consider (6.13). Here the difference of $[\Phi(n\tau + \tau/2) - \Phi(n\tau - \tau/2)] \to 1$ since the integral in (6.14)

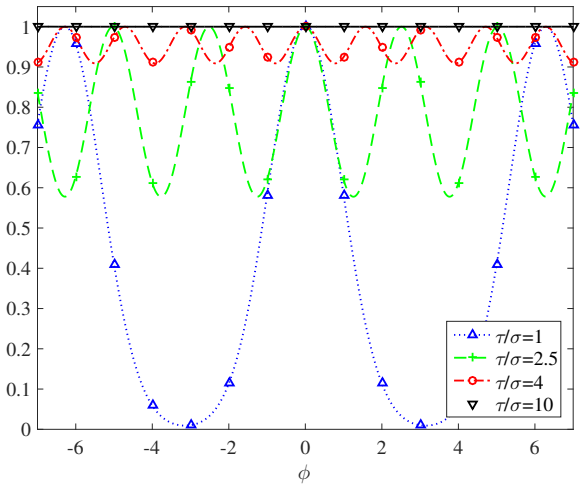


Figure 6.10. The CF as $\tau \to \infty$

as $\tau \to \infty$ for $n = 0$ is

$$\lim_{\tau\to\infty} \int_{n\tau-\tau/2}^{n\tau+\tau/2} p_{\mathcal{N}}(x)\,dx\Big|_{n=0} = \int_{-\infty}^{\infty} p_{\mathcal{N}}(x)\,dx = 1 \tag{6.27}$$

Conversely, $\forall n \neq 0$ the limit is

$$\lim_{\tau\to\infty} \int_{n\tau-\tau/2}^{n\tau+\tau/2} p_{\mathcal{N}}(x)\,dx\Big|_{n\neq 0} = \int_{\infty}^{\infty} p_{\mathcal{N}}(x)\,dx = \int_{-\infty}^{-\infty} p_{\mathcal{N}}(x)\,dx = 0. \tag{6.28}$$

Note that this relationship can be extended to any probability density function since $\Pr[x < \infty] = 1$, $\Pr[x < -\infty] = 0$ for any RV X, and since the CDF is monotonic.

Similarly, let $\tau \to \infty$ for $P_{\mathcal{N}'}(\phi)$. This time the separation between A_{n-1} and A_n will go to 0 which follows from the limit of $2\pi/\tau$ as $\tau \to \infty$. Because $P_{\mathcal{N}'}(\phi)$ is the sum over all n we find

$$\lim_{\tau\to\infty} P_{\mathcal{N}'}(\phi) = 1 \tag{6.29}$$

which is verified numerically in Figure 6.10. Here we find that the limit is reached quite quickly at around 10σ. Note also that $\forall\tau$, $P_{\mathcal{N}'}(0) = 1$ satisfying the requirement that $\int_{\infty} p_{\mathcal{N}'}(x)dx = 1$.

The result in (6.29) can be verified by taking the Fourier transform of (6.26)

$$\delta(x) \overset{\mathcal{F}}{\longleftrightarrow} 1 \tag{6.30}$$

which follows from the requirement that $p_{\mathcal{N}'}(x) \overset{\mathcal{F}}{\longleftrightarrow} P_{\mathcal{N}'}(\phi)\ \forall\tau$. Therefore, the Fourier pairs must agree at all extrema of τ.[33]

6.7 The Variance of a Quantized Random Variable

Recall that the k^{th} moment can be derived from the CF via the relationship [65]

$$\mathrm{E}\left\{\mathcal{N}'^{k}\right\} = \frac{1}{j^k}\frac{d^k P_{\mathcal{N}'}(\phi)}{d\phi^2}\bigg|_{\phi=0}. \tag{6.31}$$

We proceed from (6.31) with the CF in (6.15) and the definition (6.8). Note that because (6.8) is zero mean, then the case where $k = 2$ is equivalent to the variance (i.e., $\mathrm{E}\{\mathcal{N}'^2\} = \sigma^2$). Rather than derive a closed form solution for (6.31) we use the relationships derived in the previous section for the CF at extrema of τ in order to investigate the effect of τ on $\mathrm{E}\{\mathcal{N}'^2\}$.

Consider first the case when $\tau = 0$ such that (6.24) applies. Using (6.31) it is easy to verify that $\mathrm{E}\{\eta'^2\} = \mathrm{E}\{\eta^2\}$ since (6.23) and (6.24) hold. The result is also found directly in Appendix E through evaluating (6.31). Now let $\tau = \epsilon$ where ϵ is some positive, arbitrarily small number. Since ϵ is small it is not necessary to consider any $A_n(\phi - 2\pi n/\tau)$ where $n \neq 0$. This follows from the fact that the term when $n = 1$ is found at $2\pi/\epsilon$. If ϵ is sufficiently small then this value of this term at zero will effectively be zero. This result is proven in Appendix F. With this in mind, and for sufficiently small ϵ, the variance of $\mathcal{N}'$ is found via

$$\mathrm{E}\{\mathcal{N}'^2\} = -\frac{d^2 A_0(\phi)}{d\phi^2}\bigg|_{\phi=0}. \tag{6.32}$$

[33] Section 6.6 is revised from [29].

Using the product rule, the derivative can be evaluated as

$$\frac{d^2}{d\phi^2}P_U(\phi)P_{\mathcal{N}}(\phi) = \\ P_U(\phi)\frac{d^2}{d\phi^2}P_{\mathcal{N}}(\phi) + \frac{d^2}{d\phi^2}P_U(\phi)P_{\mathcal{N}}(\phi) \\ + 2\frac{d}{d\phi}P_U(\phi)\frac{d}{d\phi}P_{\mathcal{N}}(\phi). \tag{6.33}$$

Notice that when evaluated at $\phi = 0$ the first and second derivatives of $P_{\mathcal{N}}(\phi)$ are 0 and $-\sigma^2$ respectively. Also, note that $P_U(0) = P_{\mathcal{N}}(0) = 1$. After applying these observations and distributing the negative sign we can simplify (6.33) to

$$\left.\frac{d^2A_0(\phi)}{d\phi^2}\right|_{\phi=0} = \sigma^2 - \left.\frac{d^2}{d\phi^2}P_U(\phi)\right|_{\phi=0}. \tag{6.34}$$

This derivation is made more rigorous in Appendix E. Since $P_U(\phi)$ is concave down $\forall\tau > 0$ at $\phi = 0$ we have that

$$\mathrm{E}\{\mathcal{N}^2\} < \mathrm{E}\{\mathcal{N}'^2\} \tag{6.35}$$

where the inequality is strict for a sufficiently small and non-negative ϵ[34].

Next consider the case when $\tau = \infty$. Recall from (6.29) that $P_{\mathcal{N}}(\phi) = 1$. It can be verified that the second derivative is 0 for $\phi = 0$. This result is found explicitly in Appendix E. Thus, when τ is very large the variance of $\mathcal{N}'$ becomes very small such that the inequality in (6.35) is reversed for a sufficiently large τ.

This behavior of the variance as $\tau \to \infty$ requires that $\text{Ш}_\tau(x)$ is not shifted relative to the mean of $\mathcal{N}$. In other words, $\psi = 0$ for $\text{Ш}_\tau(x - \psi)$ in Q. The difference in $p_{\mathcal{N}'}(x)$ is shown in Figure 6.11 for $\psi = 0$ (left pane) and $\psi = \tau/2$ (right pane). Subsequently, we will show that these values of ψ are particularly important when evaluating the extrema of $\mathrm{E}\{\mathcal{N}'^2\}$.

[34]The value of the second term in (6.34) can be calculated to a high degree of accuracy using Sheppard's corrections [69] when $\tau \lesssim \sigma$ [65].

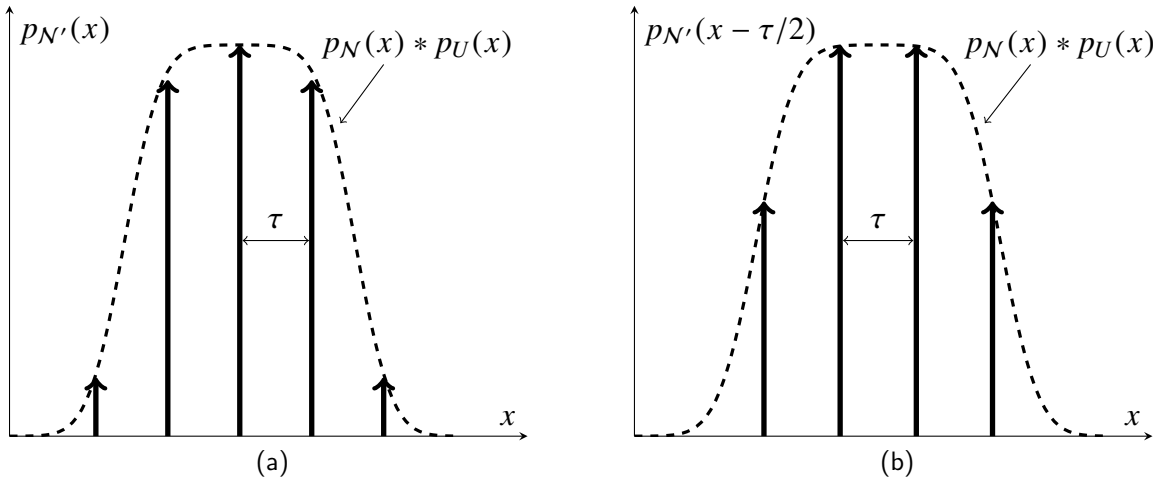


Figure 6.11. The difference in $p_{\mathcal{N}'}(x)$ for the extrema of the shift factor ψ

To continue the analysis, consider when $\psi = \tau/2$ such that

$$\mathrm{p}_{\mathcal{N}'}(x|\psi)\big|_{\psi=\tau/2} = \sum_n \alpha_{n,\psi}\delta(x - n\tau - \psi)\bigg|_{\psi=\tau/2} = \sum_n \alpha_{n,\tau/2}\,\delta(x - 3n\tau/2) \tag{6.36}$$

and again let $\tau \to \infty$. In this case, we can approximate

$$\lim_{\tau\to\infty} p_{\mathcal{N}'}(x|\psi)\bigg|_{\psi=\tau/2} = \frac{1}{2}\delta(x + \tau/2) + \frac{1}{2}\delta(x - \tau/2). \tag{6.37}$$

The proof for this result is given in Appendix E.

By inspection of (6.37), it follows then that as $\tau \to \infty$, $\mathrm{E}\{\mathcal{N}'^2\} \to \infty$. It can be shown that as ψ increases (or decreases) from $\psi = \tau/2$ for a constant τ where $\psi \in [0, \tau]$, the second moment of $\mathcal{N}'$ returns to zero. It can further be shown that these variance maxima occur for values of $\psi = k\tau + \tau/2$ which have corresponding minima at $\psi = k\tau$ for $k \in \mathbb{Z}$. For sufficiently large τ the second moment then exhibits periodic behavior with period τ. The proof for these results are given in Appendix E.

Having established that $\mathrm{E}\{\mathcal{N}'^2\}$ is periodic in ψ, let

$$\mathrm{E}\{\mathcal{N}'^2\} = \beta f(\psi, \tau) + C \tag{6.38}$$

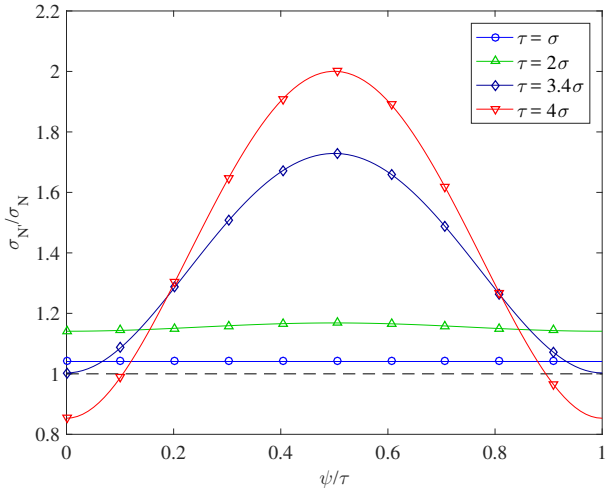


Figure 6.12. The variance of $\mathcal{N}'$ for a given shift, ψ is presented. Source: [29].

where $f(\cdot)$ is a function which is periodic in ψ with period τ. The amplitude of $f(\cdot)$ is β and has offset C. It will subsequently be useful to determine the τ for which $\mathrm{E}\{\mathcal{N}^2\} < C - \beta/2$ (i.e., the value at which the variance of the quantized RV is guaranteed to be larger than the variance of the latent RV $\forall\psi$, $\mathrm{E}\{\mathcal{N}^2\} \leq \mathrm{E}\{\mathcal{N}'^2\}$). To find this range let $\psi = 0$, which we have previously seen, is the minimum of (6.32). To make calculations more tractable we only consider $n \in \{-1, 0, 1\}$ in (6.10). Because this function is even, the value of $a_{-1} = a_1 = \Phi(-\tau/2)$. The desired bound on the variance of this probability mass can then be shown to be (cf. Appendix G)

$$2\tau^2\Phi(-\tau/2) \lesssim \sigma^2 \tag{6.39}$$

where equality holds when $\tau \approx 3.4\sigma$. Thus, we state that $\tau \lesssim 3.4\sigma$ is a necessary and sufficient condition such that the inequality in (6.35) holds $\forall\psi$.

To better illustrate the relationship between ψ and $\mathrm{E}\{\mathcal{N}'^2\}$ consider Figure 6.12. Here the shape of (6.38) is shown for various values of τ when $\psi \in [0, \tau]$. Both ψ and the variance have been normalized such that it is easier to compare the effect of τ and ψ. First, note that as τ increases the amplitude β also increases. As previously calculated, (6.38) always stays above σ_N for $\tau \lesssim 3.4\sigma$. As τ increases beyond this bound then the minimum value of the variance may drop below σ_N for certain ψ. Second, note that for sufficiently small τ (e.g.,

$\tau \leq \sigma$ in this study) the observed variance of $\mathcal{N}'$ is very close to the corrected variance of $\mathcal{N}$ which agrees with Sheppard's famous corrections [69]. However, as τ grows above σ the correction becomes less accurate. As the trend in the Figure 6.12 suggests, and the analysis has shown, for larger τ the minimum of (6.38) will eventually reach zero and the maximum will grow to infinity.[35]

6.8 Information Loss in a Quantized Random Variable

Here, following [65], we invoke the analogy of traditional sampling theory and the Nyquist rate in order to investigate injectivity in $\mathcal{N} \mapsto Q(\mathcal{N})$. Recall that when sampling a signal, the sampled output is considered representative of the input continuous-time signal if and only if the sampling rate is greater than or equal to twice the highest frequency in the continuous-time signal. If this condition is met we may say that the sampling operation is injective. Stated another way, if the former condition is met, we may perfectly recover the continuous-time signal from the sampled representation because the sampled representation contains all of the information of the original signal.

Notice the similarity between sampling and quantization. The connection is illustrated by the second step in defining Q which involved multiplication of a scaled impulsion train $\text{Ш}_\tau(x)$ with the convolved latent density. If our goal is to recover the latent density then the conditions necessary and sufficient for said recovery is of interest. Widrow's First Quantization Theorem (QT1) states that if a RV is bandlimited[36] by $\pm\pi/\tau$ then the distribution and CF of the latent RV can be perfectly recovered [70]. The implications of this theorem are far reaching, however, many real-world RVs are not bandlimited. For instance, the normal RV is an example of an extremely common RV whose CF has infinite support. Thankfully, Widrow also noticed this difficulty and showed in his Second Quantization Theorem (QT2) that an approximately bandlimited RV (relative to the bin size τ) can also be recovered with high fidelity [70]. The recovery of moments is closely related to Sheppard's correction, which is shown here for the second moment [69]

$$\mathrm{E}\{\eta^2\} = \mathrm{E}\{\eta'^2\} - \frac{\tau^2}{12}. \tag{6.40}$$

[35]This section is revised from [29].

[36]Widrow uses the term "bandlimited" to define the case when a CF has finite support [65].

Widrow offers $\tau \leq \sigma$ as a rule of thumb to define the condition necessary to satisfy QT2 [65]. The efficacy of this rule of thumb is verified by inspection of Figure 6.12.[37]

6.9 A Lower Bound for the Variance of a Quantized Random Variable

Here, we invoke the CRLB (cf. (6.1)) to show it as an appropriate lower bound for a quantized RV.

Theorem 1: *For a latent RV, parameterized by* θ

$$\mathrm{Var}_\theta\{\hat{\boldsymbol{p}}\} \geq \mathrm{CRLB}_\theta, \tau \in [0, 3.4\sigma] \tag{6.41}$$

where $\hat{\boldsymbol{p}}$ *is an unbiased estimator of theta which uses quantized observations of the RV to estimate* θ*.*

Proof: Consider the RV $\mathcal{N}$ which is then quantized with bin size τ and $\psi = 0$. If we let $\tau \to 0$ then the relationships (6.24) and (6.23) apply and the proposition becomes the standard CRLB.

Next, as τ increases from zero (6.10) can also be seen as a sum of shifted and scaled Bernoulli "pseudo-distributions". We note that each of the pseudo-distributions is not a true distribution since the resulting sum must satisfy $\int_\infty p_{\mathcal{N}'}(x)dx = 1$ and therefore $0 < \int_\infty \tilde{p}_{\alpha_n}(x)dx \leq 1 \; \forall n$ where $\tilde{p}_{\alpha_n}(x)$ is the n^{th} pseudo-distribution.

Next, recall that the Fisher information of a Bernoulli RV is given by $\mathcal{I}(p) = \sigma_b^{-2}$ where σ_b^2 is the variance of a Bernoulli RV. Therefore the Fisher information of the quantized RV is given by

$$\mathcal{I}(x') = \sum_n \tilde{\mathcal{I}}_n(p) = \sum_n \tilde{\sigma}_n^{-2} \tag{6.42}$$

where $\tilde{\sigma}_n^2$ is the pseudo-variance of the n^{th} Bernoulli pseudo-distribution.

Now we have already shown, and Sheppard's correction for the second moment (6.40)

[37] This section is revised from [29].

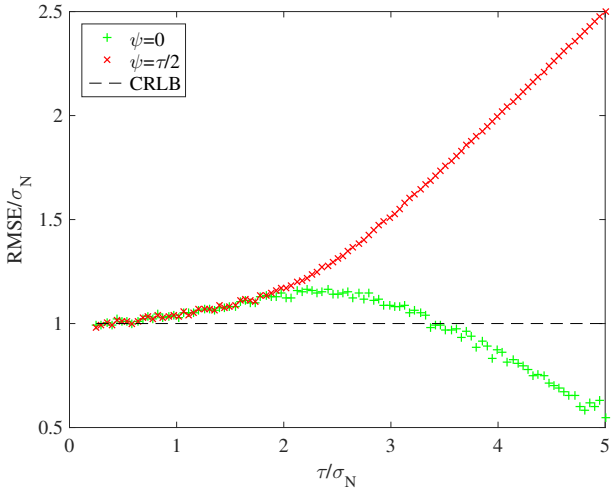


Figure 6.13. The variance of a MLE of a quantized RV parameterized by τ is presented for two different offsets ψ. Source: [29].

verifies (c.f. also Figure 6.12), that for small τ the following will hold

$$\sum_n \tilde{\mathcal{I}}_n(p) \leq \mathcal{I}(x). \tag{6.43}$$

Stated another way, the variance of the quantized signal must not be smaller than that of the latent signal. Therefore, the Fisher information of the observed RV will not be larger than the Fisher information of the latent RV and the inequality in the theorem will be strict. Similarly, we have shown that the variance of the observed RV will be greater than the original for $\tau \lesssim 3.4\sigma$ so the proposed bound will hold for $\tau \in [0, \sim 3.4\sigma), \forall\psi$. ■

To verify the theorem is valid consider a normal RV $\mathcal{N}(\mu, \sigma^2)$ which is quantized and the parameter to be estimated is the mean, μ. We show the results of a numerical study in Figure 6.13 in which we estimate μ via the standard maximum-likelihood method for various bin sizes, τ. It can be seen that for any shift in the bins (i.e., $\forall\psi$) that the resulting RMSE lies above the CRLB for $\tau \lesssim 3.4\sigma$ which supports Theorem 1. Conversely, for values of $\tau \gtrsim 3.4\sigma$, the results shown in Figure 6.13 demonstrate that CRLB will not be appropriate $\forall\psi$. Thus, without *a priori* knowledge of the exact annular offset ψ, the a lower bound cannot be realized.

Note that for smaller relative values of τ (e.g., $\tau \in [0, \sigma)$) the deviation from the latent RV

variance is minimal. Thus, it will be that the bound presented in Theorem 1 is not strict and an efficient estimator will achieve the lower bound. In other cases where τ is larger and the quantized variance deviates from the latent variance, an efficient estimator will not meet the lower bound as defined by the latent variance and the inequality in the theorem will be strict. However, for smaller τ the deviation of the quantized RV variance from the latent RV variance can be calculated with a high degree of fidelity via Sheppard's correction (6.40). Thus, the bound can be adjusted in this manner to show a tighter lower bound for larger τ and evaluate the efficiency of estimators.[38]

[38]This section is revised from [29].

THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER 7:
The Timing Advance as a Quantized Random Variable

In this section, we describe the TA as a quantized RV and compare the current RV with that of a legacy cellular protocol. We then derive a MLE and lower bound for the TA-based position estimate through showing that the LTE TA satisfies the requirements of Theorem 1.

7.1 Spatial Quantization in Cellular Networks

It is not difficult to see that the TA is a quantized RV. First, the base station must make a distance estimate based on the time of arrival of a UE's uplink frame which we model as a normal RV. The assumption of normality associated with this phenomenon is well accepted in the literature [7], [10]. Next, the eNB must determine if the measured distance necessitates adjustment to the UE's timing. Because the base station can only affect timing adjustment in discrete units, the timing mismatch must be greater than τ/c in order for an adjustment to be issued. Hence, the TA can be seen as quantizing the UE's distance from the serving eNB to the nearest multiple of τ as in Figure 7.1. Recall that, in LTE,

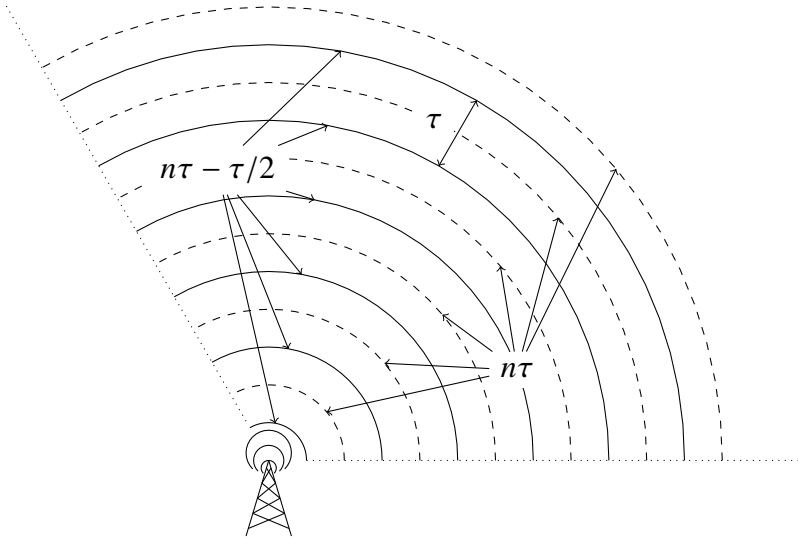


Figure 7.1. The quantization of the TA

$\tau = 78.125$ m (cf. (4.4)).

The quantization scheme depicted in Figure 7.1 is also applicable to GSM where $\tau = 550$ m [40]. The difference in quantile size for GSM and LTE can be attributed to tighter timing alignment required in LTE in order to support higher data rates. To highlight how the change in quantile size from GSM to LTE affects the statistics of the problem, let first $\sigma_{BTS} \approx \sigma_{eNB} = \sigma$. In other words, let the latent RV associated with the eNB(BTS) error estimation of the UE distance be approximately the same. Let $\sigma = 50$ m following our review of field measurements in Chapter 4. Next, recall that the lower bound associated with a quantized RV is the CRLB as long as $\tau \lesssim 3.4\sigma$ (cf. Theorem 1).

For LTE this condition holds since

$$\tau_{LTE} \approx 1.56\sigma. \tag{7.1}$$

This assures that there is a finite lower bound on the measurement error and that the error will be approximately independent from the annular offset, ψ.

Conversely, in GSM the condition does not hold since

$$\tau_{GSM} = 11\sigma. \tag{7.2}$$

Thus, the performance of the position estimate will be highly dependent on ψ. This means that if the target UE is a favorable distance away from the BTS (i.e., $d = n\tau$ so that $\psi = 0$) then the variance of the position estimate will go to zero as $\tau \to \infty$ (cf. Figure 6.13). Alternatively, if the target UE is not a favorable distance away from the BTS (i.e., $d = n\tau + \tau/2$ so that $\psi = \tau/2$) then the variance of the position estimate will become very large as $\tau \to \infty$ (cf. Figure 6.13).

Therefore, the tighter timing alignment in LTE marks a significant change in how the TA can be used for positioning. In LTE the TA can be used with relatively consistent results. Conversely, the performance associated with TA-based positioning in GSM will vary significantly since ψ is generally not known *a priori*.

7.2 A Maximum Likelihood Estimate and Lower Bound for Timing Advance Positioning

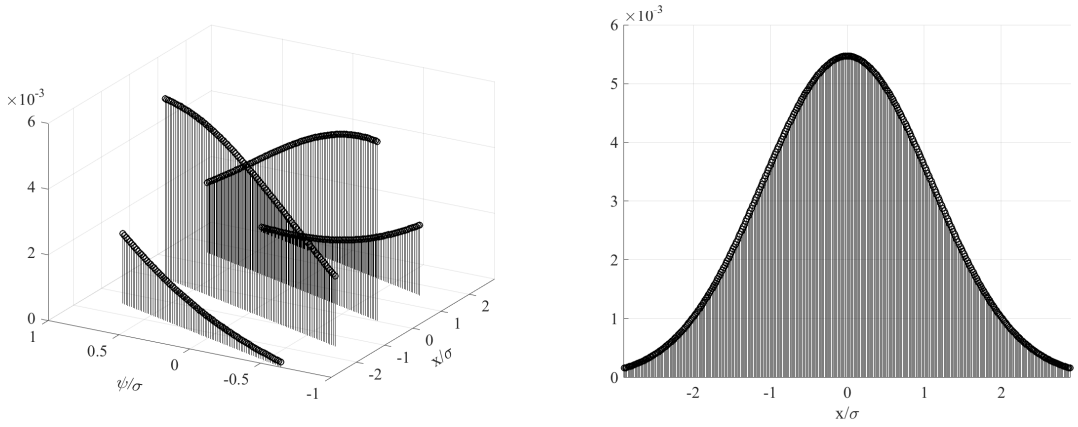
In order to derive a MLE for a UE position we must first characterize the distribution of error after quantization $p_{\mathcal{N}'}(x)$ which is shown in Figure 6.6 and given in (6.10). However, we have shown in (6.37) that the shape of the density is parameterized by ψ. Despite this fact, we will further show that it is also appropriate to model all possible $p_{\mathcal{N}'}(x|\psi)$ with a single density that is independent of ψ.

To begin, let $p_{\mathcal{N}'}(x, \psi)$ be the joint density of the error in the distance estimate and annular offset ψ. Next, let $p_{\mathcal{N}'}(x)$ be a normal marginal density of $p_{\mathcal{N}'}(x, \psi)$. Recall, that this choice of a distribution models the continuous error associated with distance measurement and is widely accepted in the literature [7], [10]. To arrive at $p_{\mathcal{N}'}(x|\psi)$, contrast the effect on $\text{Ш}_\tau(x - \psi)$ of when a UE is positioned in the center of a TA annulus ($\psi = 0$) with when a UE is on a TA boundary ($\psi = \tau/2$) which is shown in Figure 6.11. Upon inspection, it appears that $p_{\mathcal{N}'}(x)$ and $p_\Psi(\psi)$ should be dependent since the shape of $p_{\mathcal{N}'}(x|\psi)$ is completely dependent on ψ. However, it has been shown that if the conditions of QT1 or QT2 are satisfied then $p_{\mathcal{N}'}(x)$ and $p_\Psi(\psi)$ are, in fact, independent [71], [72].

The implications of this paradoxical independence on the TA as a RV is that regardless of where the UE is located within a TA annulus, the error can be modeled with the same density assuming the conditions of QT1 or QT2 can be met. This is an important fact to establish in order to make an MLE which is independent of ψ tractable. It is obvious that neither τ_{GSM} or τ_{LTE} meet QT1 since the latent, unquantized, RV (Gaussian) is not bandlimited. Fortunately, QT2 only requires approximate bandlimitation. It can be seen from (7.2) that GSM does not satisfy QT2. However, from (7.1) it can be seen that LTE does satisfy QT2.

Thus, in addition to providing consistent results from TA-based positioning, the tighter timing alignment in LTE also allows us to formulate a MLE independent of ψ allowing for tractable analysis and making a closed form solution possible.

To see this consider the joint density presented in the left pane of Figure 7.2. When the joint density is rotated such that the ψ dimension is not visible, as in the right panel, one can observe the latent normal density. If the value of ψ is completely unknown it would be



(a) $p_{\mathcal{N}'}(x, \psi)$ (b) $p_{\mathcal{N}'}(x)$

Figure 7.2. The joint and marginal density of the error associated with TA-based positioning is presented. Adapted from [29].

reasonably modeled as a uniform RV. Thus, by integrating

$$\int_{\psi} p_{\mathcal{N}'}(x|\psi) p_{\Psi}(\psi) d\psi \tag{7.3}$$

we find $p_{\mathcal{N}'}(x) \sim \mathcal{N}(0, \sigma^2)$. However, because ψ and x are independent

$$\begin{aligned} \int_{\psi} p_{\mathcal{N}'}(x|\psi) p_{\Psi}(\psi) d\psi &= p_{\mathcal{N}'}(x) \int_{\psi} p_{\Psi}(\psi) d\psi \\ &= p_{\mathcal{N}'}(x) \end{aligned} \tag{7.4}$$

therefore $p_{\mathcal{N}'}(x) \sim \mathcal{N}(0, \sigma^2)$ regardless of the shape of $p_{\Psi}(\psi)$.

Having established $p_{\mathcal{N}'}(x|\psi) = p_{\mathcal{N}'}(x)$, we can now formulate the MLE for a set of single distance measurements $\hat{\boldsymbol{d}} = [\hat{d}_1, \hat{d}_2, \ldots, \hat{d}_N]^T$ from N distinct eNBs as

$$\hat{\mathbf{p}} = \arg\max_{\mathbf{p}} p(\hat{\boldsymbol{d}}|\mathbf{d}) \tag{7.5}$$

where $\hat{\mathbf{p}} = [\hat{x}, \hat{y}]^T$ is the position estimate and $\mathbf{d} = [d_1, d_2, \ldots, d_N]^T$ is a vector of true distances such that $\hat{d}_i = d + \mathcal{N}'$. The solution to this program for normally distributed

measurement error is well-known as [10]

$$\sum_{i=1}^{N} \frac{(d_i - \hat{d}_i)(x - x_i)}{\sigma_i^2 d_i} = 0 \tag{7.6}$$

$$\sum_{i=1}^{N} \frac{(d_i - \hat{d}_i)(y - y_i)}{\sigma_i^2 d_i} = 0. \tag{7.7}$$

Solving (7.6) and (7.7) directly involves an exhaustive search in $\mathbf{p}$. However, numerical solutions have been proposed that have been shown to be statistically efficient (e.g., [31]). A further difficulty of (7.6) and (7.7) is that they depend on the true distance estimate d_i which is obviously not known *a priori*.

Here, we adopt two methods for approximating the solution to (7.6) and (7.7). In the first approach we approximate the MLE as [73]

$$\hat{\mathbf{p}} = \arg\min_{\mathbf{p}} \sum_{i=1}^{N} \left(\hat{d}_i - ||\mathbf{p} - \mathbf{p}_i||\right)^2 \tag{7.8}$$

where $\mathbf{p}_i = [x_i, y_i]^T$ is the position of the i^{th} eNB. The sum can easily be extended to include a CeSAR measurement by

$$\hat{\mathbf{p}} = \arg\min_{\mathbf{p}} \left(\hat{d}' - \| \mathbf{p} - \mathbf{p}' \|\right)^2 + \sum_{i=1}^{N} \left(\hat{d}_i - \| \mathbf{p} - \mathbf{p}_i \|\right)^2 \tag{7.9}$$

where $\mathbf{p}' = [x', y']^T$ is the position of the CeSAR sensor.

In this way, each term in the sum represents the squared residual error associated with each position in $\mathbf{p}$ given the distance measurements $\hat{\boldsymbol{d}}$. The $\mathbf{p}$ which minimizes the sum of the squared residuals is taken as the position estimate $\hat{\mathbf{p}}$. This approximation will be valid only for the case where each $\sigma_i = \sigma, \forall i$ and is thus a necessary condition. This is a well-known technique which is widely accepted, especially in the case where the error cannot be exactly parameterized by a probability distribution [10]. Note that (7.8) and (7.9) do not depend on any d_i thus removing a significant obstacle associated with (7.6) and (7.7); however, the solution to (7.8) and (7.9) cannot be found in closed form. Instead, numerical means must be leveraged which can still be computationally expensive [10].

The second solution we leverage takes more of a brute force approach which trades computational complexity for a solution which is not nuanced by idiosyncrasies associated with more complex approximate methods (e.g., the non-linear solver associated with the numerical solution to (7.8)). This solution first computes a single error surface over the tracking area. Assuming each measurement to be independent of the next it can be defined by

$$\mathrm{p}(\hat{\boldsymbol{d}}|\mathbf{p}) = \prod_{i=1}^{N} \mathrm{p}(\hat{d}_i|\mathbf{p}). \tag{7.10}$$

An optional equivalent surface, relative to the solution of (7.6) and (7.7), which may be more convenient can be expressed as

$$\tilde{\mathrm{p}}(\hat{\boldsymbol{d}}|\mathbf{p}) = \sum_{i=1}^{N} \log \mathrm{p}(\hat{d}_i|\mathbf{p}) \tag{7.11}$$

where $\tilde{\mathrm{p}}(\hat{\boldsymbol{d}}|\mathbf{p})$ is known as the log-likelihood function of $\hat{\boldsymbol{d}}$. The sum in (7.11) can be extended to include a CeSAR measurement so that

$$\tilde{\mathrm{p}}(\hat{\boldsymbol{d}}|\mathbf{p}) = \log \mathrm{p}(\hat{d}'|\mathbf{p}) + \sum_{i=1}^{N} \log \mathrm{p}(\hat{d}_i|\mathbf{p}). \tag{7.12}$$

Because the value at each point in the error surface must be computed individually, the surface necessarily will have some granularity which can be thought of as sampling. The granularity will vary inversely with the computational load. Thus, the higher the resolution of the surface, the higher the computational load. This surface is then exhaustively searched for the global maximum. A second surface, with a higher resolution and smaller area, is then calculated around this global maximum in order to refine the estimate. The global maximum on the second surface is then taken as

$$\hat{\mathbf{p}} = \arg\max_{\mathbf{p}} \tilde{\mathrm{p}}(\hat{\boldsymbol{d}}|\mathbf{p}). \tag{7.13}$$

This method, while computationally costly, will later be shown to be efficient in the sense of the lower bound derived in Chapter 7 while, similar to (7.8), not being dependent on any d_i.

A difficulty associated with each of these solutions is that a valid starting point must be used in order to avoid the local maximum trap. Therefore, we assume an *a priori* knowledge of the general target location such that the local maximum trap is avoided. In order to highlight more relevant points in the results and avoid sources of error associated with local maxima we initialize each solution with the true location of the UE. We recognize this artificiality in the experimentation while also noting that optimization of difficult objectives with local maxima is a well-traveled subject in the literature and not the focus of our research.

Finally, because the $\hat{\mathbf{p}}$ generated in this way are not exact, we hereafter refer to solutions made via one of the two aforementioned methods as the approximate-MLE (AMLE).

THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER 8:
Results

In this chapter, we present results that support the previous analysis and describe the performance of TA-based positioning with and without CeSAR augmentation. Furthermore, the ability of CeSAR to mitigate geometric weaknesses in the network infrastructure is demonstrated. We first show the accuracy of TA-based positioning and CeSAR augmentation in various scenarios using synthetic and empirical data. Next, we show the MLE to be an efficient estimator in the context of the lower bound derived in Chapter 7.

The results presented herein have been largely previously published (or are submitted for publication) [21], [24], [28], [29]. Specifically, Section 8.1.1 is revised from "Cellular Synchronization Assisted Refinement (CeSAR): A Method for Accurate Geolocation in LTE-A Networks" by John Roth, Murali Tummala, and James Scrofani published in the proceedings of the 49th Hawaii International Conference on System Sciences in January 2016 [24]. Section 8.1.2 is revised from "Location Privacy in LTE: A Case Study on Exploiting the Cellular Signaling Plane's Timing Advance" by John Roth, Murali Tummala, John McEachen, and James Scrofani to be published in the proceedings of the Hawaii International Conference on System Sciences in January 2017 [28]. Section 8.3.2 is revised from "On Location Privacy in LTE" by John Roth, Murali Tummala, John McEachen, and James Scrofani which has been submitted for publication [29].

8.1 Accuracy of Timing Advanced-Based Positioning

In this section, we use synthetic and empirical data to examine the achievable accuracy associated with TA-based positioning and CeSAR augmentation.

8.1.1 Synthetic Results

First, using only synthetically generated measurements we evaluate performance in several scenarios of interest. Specifically, we investigate performance in legacy deployments, handover scenarios, and in heterogeneous networks. When CeSAR is included, no error is assumed in the CeSAR measurement and the most central point on the refined locus is used

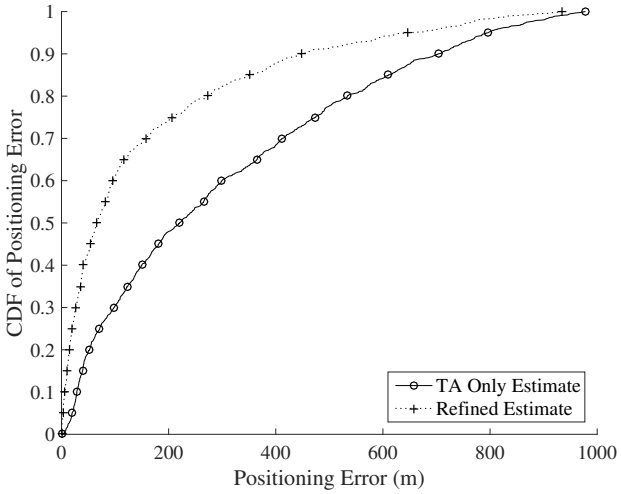


Figure 8.1. Results of positioning with synthetic data in a legacy network deployment is presented. The refined estimate is the result of CeSAR augmentation. Source: [24].

as the position estimate. When CeSAR is not used, the centroid of the locus is used as the position estimate. Additionally, sectoring of the serving cell is not assumed in any study. Excerpts from this section are taken from [24].

Legacy Deployments

First, we present results in several different scenarios realized with entirely synthetic measurements. In this section, TA error is modeled as uniform $\mathcal{U} \sim [-78.125/2\text{ m}, 78.125/2\text{ m}]$ and the target and sensor are randomly placed throughout the coverage area (max distance ≈ 500 m) such that the distance from the PCell is uniform as is the angle from the abscissa. It additionally imposed that the sensor-UE distance is ≥ 78.125 m. The first study uses only one serving eNB (PCell) in order to model performance in legacy LTE networks. When a position estimate is made with TA data only $\hat{\mathbf{p}}$ is chosen randomly inside the TA annulus such that the polar angle is uniformly distributed $\in [0, 2\pi)$ and annular offset ψ is uniformly distributed $\in [n\tau - \tau/2, n\tau + \tau/2]$. The results are presented via a cumulative distribution of errors in Figure 8.1.

The low performance in this technique can be explained by the high degree of uncertainty offered by a large locus. Small errors are representative of scenarios when the TA quantity is

small (i.e., the UE is physically close to the eNB) or in the unlikely scenario that the estimated position is chosen very near to the actual target location. Large errors are accounted for by large TA values (i.e., the UE is near or on the cell boundary) and when the estimated position is chosen on the opposite side of the annulus as the true target location. Of special note is this curve's very uniform appearance with the slight non-uniformity accounted for by the non-linear shape of the locus.

The second curve presented in Figure 8.1 contrasts the performance improvements that can be realized through CeSAR. This curve presents in much more of an exponential distribution, shifting the preponderance of errors to much lower values. Here, CeSAR results in 254 m improvement in the circular error probable (CEP) 70% metric.

Despite significant improvement from the former method, notable large errors are still present. These large errors are realized when the intersection between the circle and annulus results in two separate line segments (disjoint locus) and the estimated target location is on the opposite segment from the actual target location. Again, larger TAs result in the potential for larger errors, thus cell size can be linked to accuracy.

Handover Scenarios

In the next study, still in keeping with legacy network deployments, we investigate the performance of TA-based positioning during handover events. The handover scenario is particularly interesting since two TAs are issued from neighboring eNBs to the same UE within close succession of each other thus providing additional information when forming the system of equations used to generate a position estimate.

For this study, we assume that the UE is located on the cell boundary between two eNBs as defined by $\mathcal{N}(\mu_{cb}, \sigma_{cb}^2)$ where $\sigma_{cb} = 70$ m and μ_{cb} is the exact cell boundary. This model is used in order to take into account the fact that handovers do not always happen precisely at cell boundaries. The value of $\sigma_{cb} = 70$ m is chosen to be slightly larger than measured errors in eNB distance measurements (cf. Chapter 4).

As can be seen in Figure 8.2, we see a significant improvement in performance both with and without CeSAR from the previous scenario. This improvement is directly attributable to the extra positioning information associated with the second eNB. When this extra information

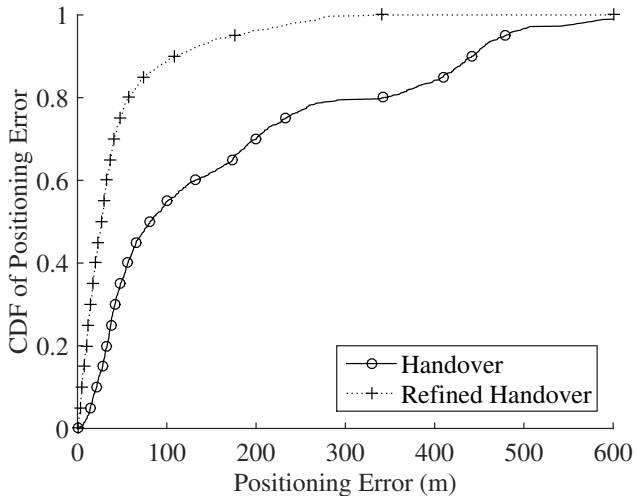


Figure 8.2. Results of positioning with synthetic data in handover scenarios is presented. The refined handover is the result of CeSAR augmentation. Source: [24].

is augmented by CeSAR the improvement becomes even more dramatic. The CEP 70% is 200 m without CeSAR and 41 m with CeSAR. Most notable, however, is the large improvement afforded by the extra information associated with the second eNB.

Heterogeneous Deployments

Motivated by the results realized in the previous section by including a TA from one additional eNB, we investigate the achievable performance possible in heterogeneous deployments. Recall (cf. Chapter 4) that LTE release 11+ deployments may include physically disparate eNBs known as SCells which simultaneously provide service to a single UE. Because there is no requirement that the eNBs are near each other, each eNB is responsible for maintaining timing alignment with the UE by issuing separate TAs attributable to the respective PCell or SCells via the TAG [50], [54].

In order to model this type of deployment, the sensor and UE locations are randomly chosen as before. The first SCells positions are chosen with distribution $\mathcal{N}(\boldsymbol{\mu}_{UE}, \sigma_{hn}^2)$ where $\boldsymbol{\mu}_{UE} = [x_{UE}, y_{UE}]^T$ is the location of the UE randomly chosen *a priori* and $\sigma_{hn} = 200$ m. This model is adopted in order to add realism to the simulation since UEs are more likely to be associated with SCells which are nearby. Additionally, the SCells will likely have a

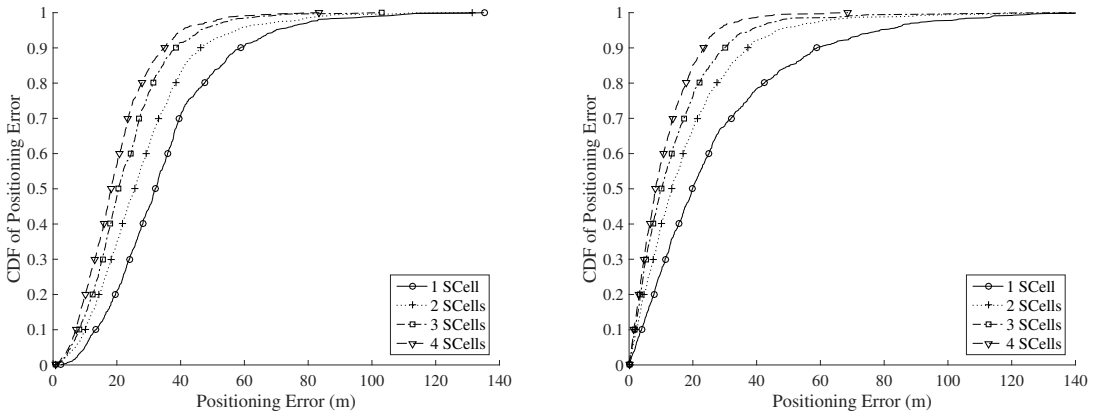


Figure 8.3. The results of positioning with synthetic measurements within a heterogeneous network deployment is presented when one to four SCells are configured along with the PCell. The results in the left pane are from TA-only positioning while those in the right pane are CeSAR augmented. Source: [24].

smaller coverage area represented by σ_{hn}. The results of varying the number of configured SCells from one to four is presented in Figure 8.3 without CeSAR in the left pane and with CeSAR in the right pane. A maximum of four SCells is considered since that is the maximum number of SCells the standard is designed to support (cf. Figure 4.2).

In the case of TA-only positioning the CEP 70% ranges from 39.7 m with one SCell configured and 23.5 m with four SCells configured. For CeSAR augmented positioning the CEP 70% ranges from 32 m with one SCell configured to 14 m with four SCells configured. For both regular and CeSAR augmented TA-based positioning, this marks a significant improvement from single eNB legacy networks. We also see that CeSAR continues to deliver performance gains even in deployments with many serving eNBs although the magnitude of the performance gains are on the order of 10 m as opposed to legacy networks where the improvement could be as large as 150 m. Finally, of note is the difference in the shape of the error distribution between CeSAR augmented and TA-only positioning. The CeSAR augmented errors appear approximately exponential while those that result from TA-only positioning have a Rayleigh-like shape. Thus, CeSAR augmentation will realize more small errors than the TA-only option.

Summary of Synthetic Results

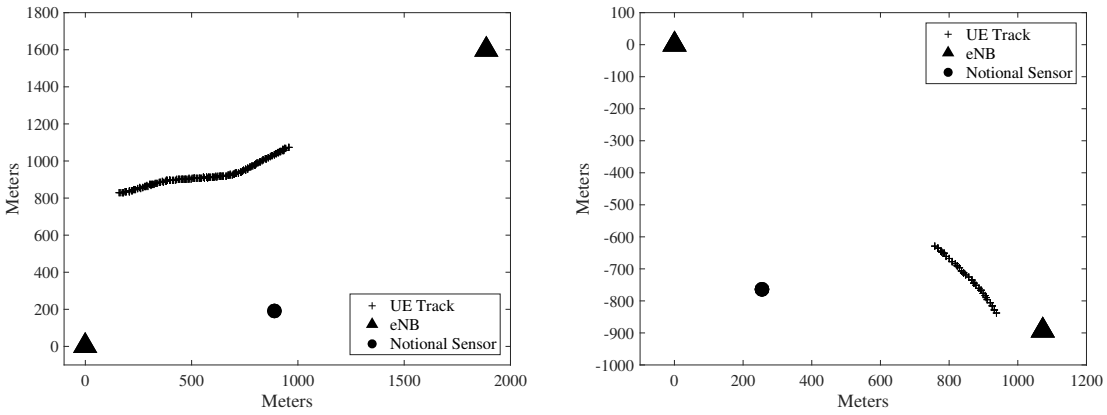
In legacy single PCell deployments with no cell sectoring we found that the CEP 70% accuracy was 412 m when only the TA was used for localization. When the position estimate was made during a handover scenario, the TA-only accuracy improved to 200 m CEP 70%. Finally, in heterogeneous networks that accuracy further improved to 39.7 m - 23.5 m for one to four SCells configured respectively.

With CeSAR augmentation, we have demonstrated that, in non-sectored cells, a user could be reliably located during normal legacy intra-cell mobility management to within 158 m, a 254 m improvement over TA-only positioning. Inter-cell mobility management showed an accuracy of 41 m, an improvement from TA-only positioning of around 159 m. In advanced heterogeneous LTE deployments the multiplicity of TAs issued to a target UE improve positioning accuracy dramatically. Here, CeSAR can deliver excellent performance on the order of 14 meters although the performance gains are not as significant as in legacy network scenarios.[39]

8.1.2 Empirical Results

In this section, we present two case studies conducted in Monterey, CA in existing LTE network deployments. In both cases, real-world TA data observed in the network are used and the position estimate is made offline. Both scenarios, depicted in Figure 8.4, include two actual serving eNBs and a notional sensor if CeSAR augmentation is used. In both cases, the track taken by the UE is shown alongside the infrastructure. Scenario A (cf. Figure 8.4, left pane) includes a UE track that is 277 m long and includes 73 recorded TAs in the 700 MHz and 2000 MHz bands. Scenario B (cf. Figure 8.4, right pane) includes a UE track that is 830 m long and includes 323 recorded TAs in the 700 MHz, 1900 MHz, and 2000 MHz bands. Both scenarios are conducted in suburban settings free from major physical obstructions like skyscrapers or other dense urban clutter. Also, in both scenarios, the UE is traveling at $\approx$ 50 km/hr. In the event that CeSAR augmentation is used, a notional sensor is included as in Figure 8.4. CeSAR measurements are modeled with normal zero-mean error with σ_c = 20 m. In both scenarios, the position estimate is calculated via the AMLE in (7.8) or (7.9).

[39]This section has been revised from [24].



(a) (b)

Figure 8.4. The infrastructure and tracks used in two case studies conducted in Monterey, CA is presented. Source: [28].

At the time of this study, the tested network did not support physically disparate carrier aggregation. Therefore, simultaneous TA issuance was simulated in the field by locking a field test phone to one eNB, driving the track depicted in Figure 8.4, then locking the phone to a neighboring tower and driving the track again. TAs were elicited and the phone was kept in the `RRC CONNECTED` state by continuously sending ping requests throughout the test drive.

The results of the above two scenarios are shown in Figure 8.5. In terms of CEP 70%, scenario A was accurate to 240 m and scenario B was accurate to 295 m. In both scenarios, CeSAR augmentation improved positioning accuracy. The CEP 70% metrics improved after augmentation to 95 m and 157 m respectively. In both scenarios, results roughly matched the positioning accuracy predicted in simulation during a handover scenario above. This is remarkable, especially given that the network performance was stretched by forcing a connection with a certain eNB while traveling outside of its normal coverage area.

This study corroborated previous simulation performance in handover scenarios in an existing LTE network in Monterey, CA. Moreover, real-world data were used to present a realistic picture of the accuracy possible with TA-only and CeSAR augmented positioning. CeSAR augmentation was further validated by demonstrating performance enhancements

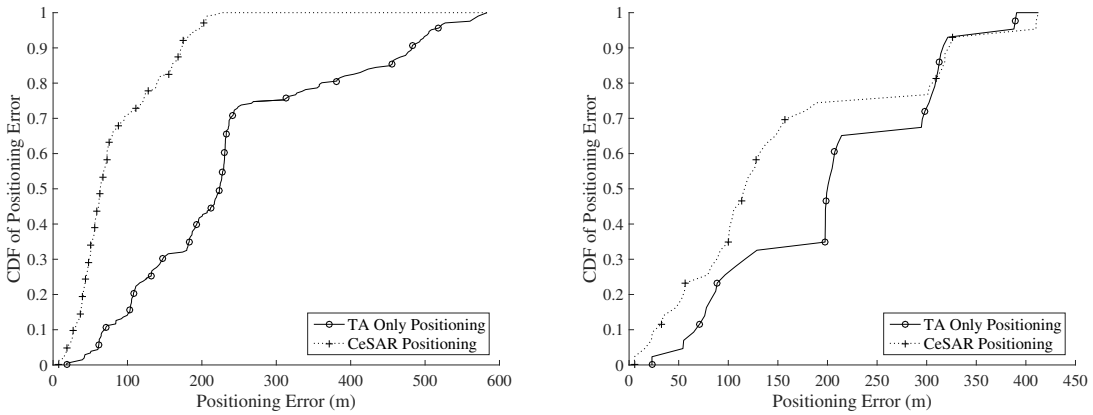


Figure 8.5. Positioning performance achieved during the case studies performed in actual network deployments in Monterey, CA. Source: [28].

of around 150 m.[40]

8.2 Empirical CeSAR Validation

In this section, we evaluate the performance of CeSAR in terms of CEP with data exclusively collected during experimentation. As before, TA data are collected from a nearby serving eNB and processed in accordance with the aforementioned precepts. The main contribution of this experiment is to introduce real-world CeSAR data.

8.2.1 Experimental CeSAR Setup

As depicted in Figure 8.6, all steps of the CeSAR method are tested with the exception of sensor-network synchronization which is assumed *a priori*. The observation of TAs is conducted as before with a field test phone. Observation of uplink bursts is conducted on-site in SDR. Finally, the sensor-UE distance estimate is made as before in the MLE with the assumption that the CeSAR error is normally distributed.

Of these steps, observation of uplink bursts is the most involved and represents the most significant contribution made by this experiment, which separates it from previous experimentation where CeSAR ranging data are synthesized. The sensor hardware implementation

[40]This section has been revised from [28].

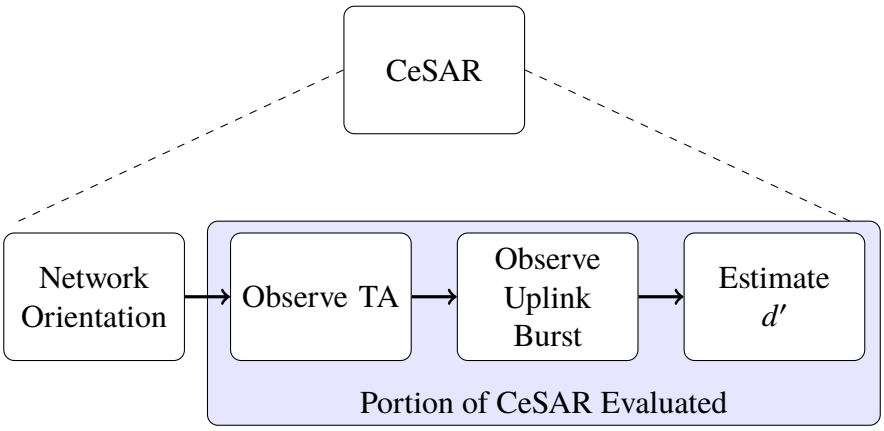


Figure 8.6. The CeSAR algorithm in field experimentation

is as presented in Section 5.2 (cf. Figure 5.2) and the overall system setup is as shown in Figure 8.7. A single USRP was used to transmit and receive a simulated UE uplink frame. The time-of-flight of the frame was measured and used to estimate the sensor-UE distance. The transmit antenna was placed in the transmit location and the USRP was collocated with the receive antenna at the receive location. The transmit antenna was connected to the USRP via a 150 m coaxial cable. Additionally, several amplifiers were used in the system to overcome losses associated with propagation along the coaxial cable and through free space. The link budget, along with a detailed system diagram is given in Appendix H.

A single USRP with synchronized TX/RX chains was used due to difficulties associated with synchronizing physically disparate USRPs. When synchronizing USRPs via GPS disciplined oscillators the best achievable synchronization had a standard deviation of ≈ 40 μs. This magnitude of synchronization mismatch translated to 12 km and was judged untenable for the application. Conversely, synchronization among TX/RX chains resident on the same SDR daughterboard resulted in errors of no more than 40 ns. Thus, intra-device synchronization was used.

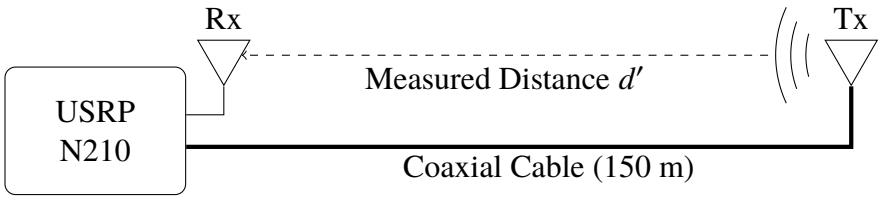


Figure 8.7. The experimental CeSAR system setup

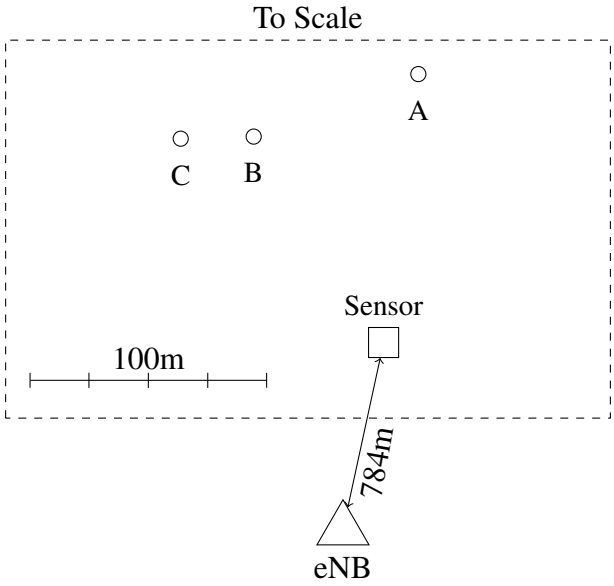


Figure 8.8. The field CeSAR test site depicted above is located in Monterey, CA. Distances inside the dashed box are drawn to scale; however, the relationship of the eNB to the local test site is not.

The time-of-flight calculation was made by transmitting a binary phase-shift keyed (BPSK) pseudo-noise (PN) sequence and matched filtering the received signal. The PN sequence was generated by a Galois linear feedback shift register (LFSR) of order 12 (4095 chips long). This length was chosen as a trade-off between maximizing the processing gain and minimizing the processing time. The signal was generated with the GNU Radio software platform[41]. While an uplink frame in LTE would be modulated by orthogonal frequency-division multiplexing (OFDM), the choice of BPSK modulation can be seen as a conservative choice when estimating performance since it will be more affected in a fading channel than its OFDM realization. The BPSK signal was transmitted at 915.1 MHz in order to simulate cellular frequency propagation characteristics while still operating in an unlicensed band. The sample rate of the N210 was set to the maximum allowable rate, 25 MSps. This sample rate maximized the final resolution of the scheme to $1/25$ MSps = 40 ns which translates to roughly 12 m.

The field test site is shown in Figure 8.8. Due to its the location, there was only one available

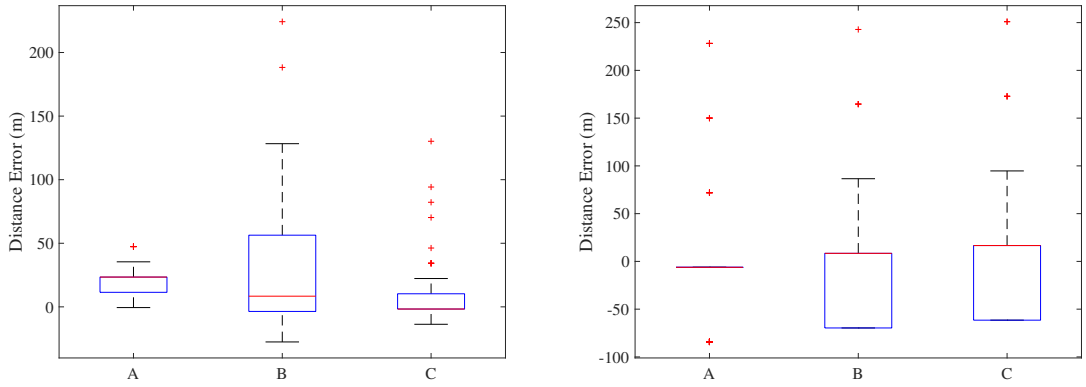
[41]See Appendix I for the python code used to synchronize the TX/RX chains and generate the transmitted signal.

serving eNB. This eNB is shown in Figure 8.8 (not to scale) three quarters of a kilometer south of the test site. The sensor remained stationary throughout the experiment and the target was moved to each of three locations: A, B, and C. At each location the sensor measured the UE-sensor distance as outlined above 100 times and received TAs from the serving eNB. Measurements were validated by ensuring the value of the correlation peak resulting from the matched filter was sufficiently high. Only one measurement taken at site A was a statistical outlier and discarded. 101, 74, and 80 TAs were collected at sites A, B, and C respectively after statistical outliers were discarded. The operating bands used while these TAs were issued were 700 MHz and 2000 MHz. As previously mentioned, the eNB bias was assumed *a priori* and taken into account when estimating d_1. The distribution of the TA and CeSAR measurements are presented in box plots in Figure 8.9.

We note that this particular experimental setup, by the nature of physical constraints (e.g., the available serving eNBs and the length of the coaxial cable), is an example of a pathological geometry (cf. Chapter 6). In these experiments $\sigma_{\text{TA}} \approx 68$ m for TA data and $\sigma_{\text{sen}} \approx 23$ m for sensor data. Therefore, assuming worst case σ, the test sites should be at least $3\sigma_{\text{TA}}$ off the symmetry directrix described by the sensor and eNB to prevent measurement bias, however, the length of the coaxial cable would not allow this, thus forcing pathology (i.e., bias) in the setup. The bias was manifested here due to the circles representing distance estimates not intersecting (cf. Chapter 6). This resulted in a preponderance of the estimates lying on the directrix. Thus, because the geometry is pathological it cannot be compared to the lower bound previously derived.

8.2.2 Empirical CeSAR Results

The measurements were used offline to calculate the position estimate and the results are presented in Figure 8.10. Because only two anchor points are used during the calculation (i.e., the sensor and the eNB), the system of equations represented by $\hat{\boldsymbol{d}}$ is underdetermined. Additionally, the proximity of the sites to the sensor makes the geometry pathological as described in Section 6.3, thus the estimate is found with the residual error method (cf. (7.8)). The results, in terms of CEP 70%, were 53.6 m, 77.3 m, and 57.8 m for locations A, B, and C respectively. The mean values were 60.7 m, 74.3 m, and 61.6 m for sites A, B, and C respectively. The curves show that the vast majority of the errors are small, however, a significant tail is also observed indicating infrequent, but large errors. Regardless, a



(a) CeSAR (b) TA

Figure 8.9. Box plots of empirical CeSAR validation measurements

level of accuracy which may be able to meet the FCC's E-911 mandate is demonstrated. Considering that in this experiment $\hat{\boldsymbol{d}}$ is underdetermined (two equations), CeSAR presents as a viable option to satisfying federal standards[42].

8.3 Efficiency in Timing Advanced-Based Positioning

An estimator is said to be efficient if it asymptotically attains the CRLB [48]. In other words, an efficient estimator will be able to attain the CRLB with an infinite number of corrupted observations. In this section, we show that TA-based location estimation can be efficient and demonstrate the maximum achievable bounds for this type of positioning with synthetic and real-world TA data. Note that since, for LTE, $\tau \approx 1.5\sigma$ Sheppard's correction is used when calculating the CRLB[43].

8.3.1 The Effect of N and the NLoS Channel

In the first study, we position notional eNBs on a scaled circle centered around the target UE as in Figure 8.11. Since the positioning accuracy is dependent only on the angular geometry and not the target-eNB distance (cf. (6.5)), the radius of the circle is some

[42]The FCC's E-911 mandate requires that $\Pr[\| \mathbf{p}_0 - \hat{\mathbf{p}} \| \leq 100\,\text{m}] = 0.67$ and $\Pr[\| \mathbf{p}_0 - \hat{\mathbf{p}} \| \leq 300\,\text{m}] = 0.95$ [4], [5].

[43]Refer to the discussion of Theorem 1 in Chapter 6 for more information on the necessity of this when showing the efficiency of an estimator using quantized observations of a RV.

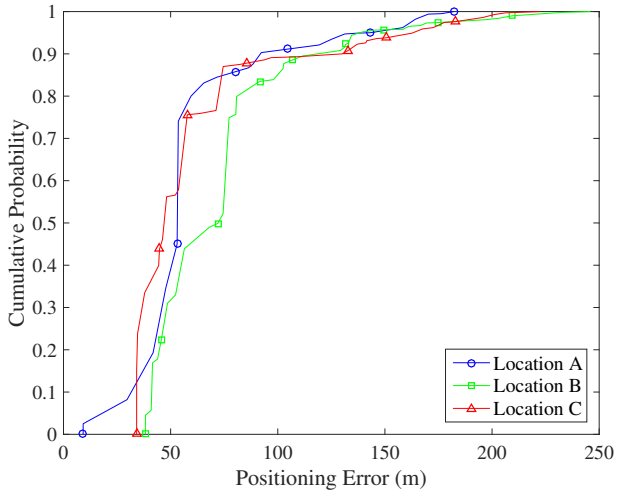


Figure 8.10. CDF of positioning with empirical CeSAR measurements

arbitrary distance r. Each eNB has a fixed angular separation of $2\pi/(N_{max}+1)$ from the next as in Figure 8.11. The study is repeated for a different $N \in \{3, 9\}$ such that the angular separation $\theta = 2\pi/(N_{max}+1)$ is held constant and the number of eNBs N is varied up to $N_{max} = 9$. When positioning is augmented with CeSAR, the sensor is placed at $\theta = -\pi(N_{max}-N)/(N_{max}-1)$. Heuristically, the CeSAR angle can be seen as being placed π radians from the center of the total angle subtending all eNBs. In order to show the effect of an NLoS channel, each eNB is optionally contaminated with NLoS error. The overall ratio of eNBs contaminated by NLoS error is given by ζ (the notation ζ^c indicates CeSAR is used). Here, NLoS error is modeled as $\delta(\hat{d}-\mu)$ in accordance with the channel model presented in Chapter 2 [7], [27], [30]. For these simulations $\mu_i = \mu = 50$ m, $\forall i$. The results of Monte Carlo trials with each N, with and without CeSAR, and for different ζ, are shown in Figure 8.12. In this case, position estimates are calculated with the AMLE presented in (7.11) and (7.12).

The left pane of Figure 8.12 first demonstrates the efficiency of the AMLE due to its congruence with the CRLB[44]. We also see that for these geometries, RMSE accuracies from ≈70 m to ≈35 m are possible. It is evident that, at first, increasing N realizes significant gains which become less significant as N becomes large relative to N_{min}. As ζ is

[44]The CRLB here and in the subsequent study have been adjusted using Sheppard's correction for quantized RVs such that $\sigma^2_{\text{CRLB}} = \sigma^2_{\text{latent}} + \tau^2/12$.

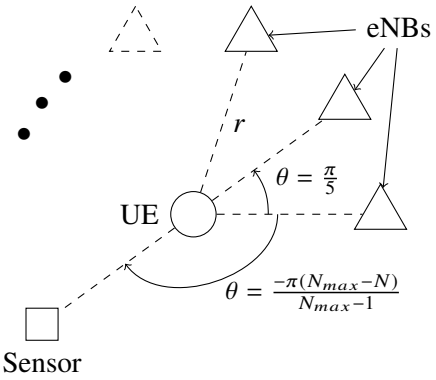


Figure 8.11. The experimental setup for real-world TA data

increased, as expected, performance decreases and the channel model prevents an unbiased estimate; hence, the CRLB is not attained. However, it is notable that even in heavy NLoS environments ($\zeta = 2/3$) RMSE accuracies of ≈95 m to ≈50 m are possible.

The right pane of Figure 8.12 shows the performance as RMSE with and without CeSAR augmentation for two levels of NLoS contamination ζ. In both cases CeSAR provides modest gains of approximately 5 m. When NLoS contamination is increased to $\zeta = 1/3$, performance decreases overall by 10 to 20 m and the relative performance increase of CeSAR remains constant. For both cases of ζ, the modest increase in performance is explained by the minimal effect of change on the angular geometry when the CeSAR sensor is included. Because the sensor is placed roughly parallel to the mid-line axis of the eNBs, CeSAR has a limited contribution (cf. (6.5)). We will show in the next experiment how the sensor can be placed in order to maximize its effect.

Finally, note that in both panes the magnitude of location accuracy demonstrated is well under that of τ. To understand this, first consider the case when $N = 1$ and when the eNB can perfectly determine the UE distance. Here, the error in the distance estimate is minimized when $\hat{\mathbf{p}}$ is chosen at the middle of the TA annulus such that the error is uniform, $\mathcal{U} \sim [-\tau/2, \tau/2]$. From this it can be shown that the associated mean error is $\approx$ 19 m and the associated RMSE is $\approx$ 22 m. Thus, the demonstrated accuracy is well above the minimum distance estimation accuracy. However, we also note that, assuming no restriction on $N_{\max}$, it is conceivable to obtain RMSE accuracy lower that 22 m when GDoP < 1 (cf. Chapter 6).

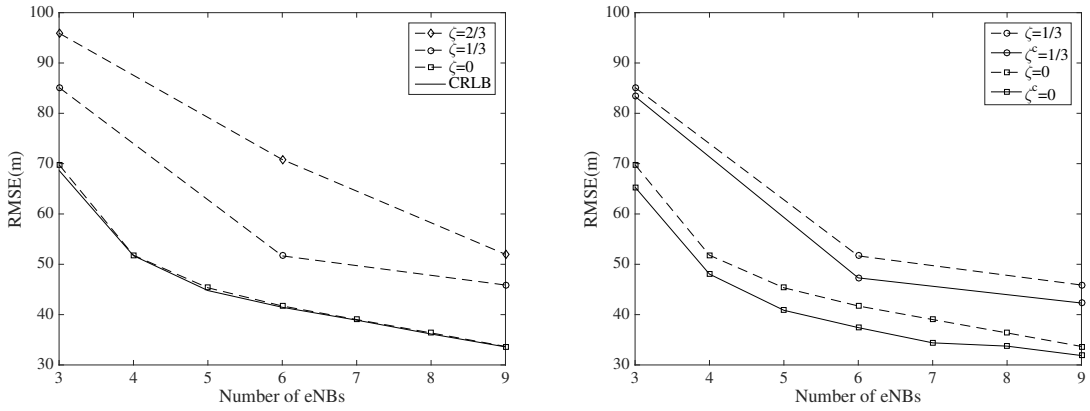


Figure 8.12. The performance of the TA-based MLE in various levels of NLoS contamination ζ with optional CeSAR augmentation (ζ^c). Source: [74].

8.3.2 The Effect of Infrastructure Geometry

We now change the experimental setup to that shown in Figure 8.13 in order to examine the efficiency of the AMLE with real-world TA data and to highlight the capacity of CeSAR to negate poor GDoP effects. In all studies, there are $N = 3$ eNBs arranged on a circle centered on the UE of some radius r. The eNBs all share an angular separation of θ. When the CeSAR sensor is used, it is positioned at $\theta = 3\pi/4$ also on the same circle with radius r. For each scenario a different angular separation between the eNBs $\theta \in \{\pi/10, 3\pi/20, \pi/5, \pi/4\}$ is used. Note that θ starts off small such that the eNBs are tightly clustered and share a similar angle to the UE. At $\theta_{\max} = \pi/4$ the third and first eNB are separated by $2\theta = \pi/2$ and the eNBs are more dispersed than at $\theta_{\min} = \pi/10$. Because in an actual LTE network deployment the number of serving eNBs and σ do not vary significantly, here we show positioning accuracy as a function of infrastructure geometry by iterating through the various values of θ. This experiment is conducted with both synthetic and real-world data. For synthetic TA data, in line with field measurements presented in Chapter 4 [21], the observed $\sigma \approx 50$ meters for all serving eNBs. Also in accordance with Chapter 7, the latent data are quantized by $\tau = 78.125$ meters before producing a distance estimate via (7.11). When the real-world data are augmented with CeSAR, the CeSAR error used is the same that was generated during the Empirical CeSAR validation presented in Section 8.2. Additionally, the same AMLE as was used in the previous experiment is also used here.

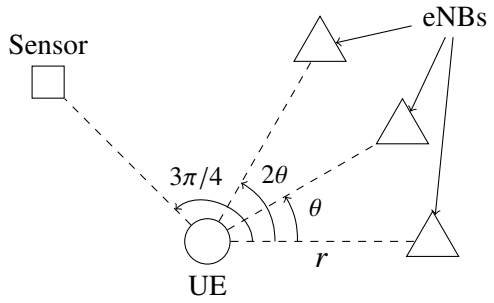


Figure 8.13. The experimental setup for all real-world TA data. Source: [29].

The results of these studies, with and without CeSAR augmentation, are presented in Figure 8.14 alongside the theoretical lower bound derived in Chapter 7 for each θ. Additionally, for each θ, real-world and synthetic data are used. First, we observe close agreement with the results and the theoretical lower bound for both synthetic and real-world data further validating the analysis and the efficiency associated with the AMLE. Second, we see close agreement between the simulated data and real-world data. This agreement validates assumptions we have made regarding the nature of the data in general which follow from the theory of quantized random variables.

Note the trend of localization accuracy. When θ is small and CeSAR is not used to augment the position estimate, the RMSE is relatively high. However, as θ increases to its maximum value, the RMSE decreases. This agrees with the trend expected given in (6.5). Thus, the existing network geometry is seen as a strong influence on the positioning performance. In this study, the accuracy varies on the order of 50 meters depending on the infrastructure layout. However, when the CeSAR sensor is included and strategically placed, the dependence of localization accuracy on network geometry can be essentially negated. This illustrates one of the main strengths of CeSAR enumerated in Section 8.2 in mitigating the effects of poor network geometry. The strategy used to maximize the geometric effect of CeSAR is to place the sensor as orthogonal to the remaining eNB angles as possible. Finally, we demonstrate with real and synthetic data that RMSE accuracies on the order of 40 meters are possible which agrees with previous studies.

Through the two studies presented here, we have shown the AMLE to be efficient relative to the CRLB. We have also demonstrated theoretical accuracies on the order of tens of meters, shown how accuracy is affected in NLoS scenarios, for various N, and demon-

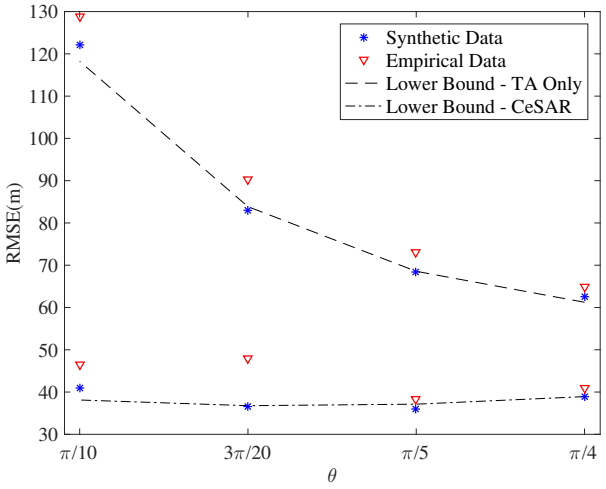


Figure 8.14. The results of the numerical studies for constant N in terms of RMSE are presented in this figure. Results realized from simulated and real-world error data are presented. Source: [29].

strated CeSAR's resilience in network infrastructure where geometry negatively affects precision.[45]

[45]This section has been revised from [29].

THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER 9:
Conclusion

In this work, we have evaluated the TA parameter as a means to position estimation in cellular networks. This investigation has shed light on the TA both as a security vulnerability and under-leveraged network parameter alike. Additionally, we showed how more information can be extracted from the TA in order to provide a refined estimate through the CeSAR method.

The investigation was conducted through protocol analysis, statistical analysis, simulation, and field experimentation. The method of evaluation began with protocol analysis where it was found that TA-based geolocation and a method of refinement, via CeSAR, was possible. Next, the position estimate as gleaned from the TA was statistically analyzed in order to determine the feasibility, in the sense of accuracy, of the method. Significant statistical findings led to simulations under various scenarios of interest such as legacy network deployments, handover scenarios, and heterogeneous network deployments. Next, field experimentation was conducted in real-world network deployments. These experimentation results uncovered parameters associated with real-world TA issuance such as error distribution shape and statistics. These real-world errors were used in simulations to demonstrate the statistical efficiency of TA-based positioning and further investigate performance. Finally, CeSAR was also investigated in a real-world wireless channel in an SDR testbed.

9.1 Significant Contributions

The results of this work have made several notable contributions. Specifically, those contributions include protocol analysis leading to the CeSAR refinement method, framing the TA as a quantized random variable to derive a MLE and corresponding lower bound on positioning error, and extensive experimentation, which included field data, that validated analytical results.

9.1.1 Cellular Synchronization Assisted Refinement

The contribution of the CeSAR method was realized from an in-depth analysis of the LTE protocol. In this analysis, it was discovered how the TA value could also be *passively* leveraged to find the UE distance from a local sensor. When combined with the traditional eNB-UE distance, which is more explicit in a TA, this information added a crucial dimension to the system of equations otherwise typically used in TA-based positioning. The protocol was also used to show that the observation needed in CeSAR was feasible without the need to bypass encryption making the contribution of CeSAR even more potent. A corollary of CeSAR was that the reconfigurable nature of the method also allowed the user to mitigate problems associated with GDoP.

CeSAR was framed as both a security vulnerability and a network performance multiplier. From the perspective of a security vulnerability, the CeSAR operator would be a third party extra-network operator. It was shown how this operator could locate a target reasonably accurately with a low chance of detection since the method is entirely passive. Conversely, from a network perspective, the method was shown to be a performance multiplier since, in contrast to current positioning protocols (cf. LPP), it is passive and does not introduce additional network traffic in developing a position estimate.

9.1.2 Statistical Analysis of the Timing Advance

The analysis of the TA first began in the LTE protocol where TA behavior such as uncertainty, issuance frequency, and reasons for issuance were investigated. Once the TA was found as a tenable means for positioning, it was next analyzed statistically by casting it as a quantized RV. This was the impetus for several important ideas.

First, it was shown in Theorem 1, that regardless of the target position within a TA annulus ψ, the latent normal error distribution could be used to model the associated error. This is significant since the exact observed error distribution is discrete, making further useful analysis untenable. However, due to the result of Theorem 1, an exact MLE for TA-based positioning was shown to be equivalent to the MLE for normally distributed error. A direct and significant consequence of the MLE, which was expressible in closed form, was a lower bound on the RMSE of the TA-based position estimate.

While the MLE was significant, we noted that it was dependent on information not likely

known *a priori* and levied a heavy computational burden to evaluate. Therefore, an AMLE was developed to demonstrate efficiency in TA-based positioning. The efficiency was shown with both simulated and real-world TA data. Demonstrable efficiency then allowed us to use the lower bound to predict asymptotic behavior of TA-based MLE positioning.

Also, notable was the comparison of the statistics of the TA in GSM versus LTE. We showed that, under certain assumptions, Theorem 1 did not apply to the TA in GSM whereas it does in LTE. This was significant because it shows that the tighter alignment required in LTE ultimately also steered the protocol around a statistical corner where not only is better accuracy possible, but the accuracy will be consistent regardless of the UE position within the TA annulus. In contrast, this consistency cannot be expected in GSM and the accuracy of the position estimate will show strong dependence on the annular offset.

9.1.3 Field Experimentation

The first goal of field experimentation was to understand how the TA behaves in the wild in order to develop a better TA model in simulation. To this end, TAs were collected in four cities spanning the east and west coasts of the United States. TAs were observed in real-world network deployments in Baltimore, MD, Annapolis, MD, San Diego, CA, and Monterey, CA. The TAs were observed in environments spanning suburban to dense urban environments, across several bands, and for stationary and moving UEs. This allowed us to validate *in situ* that the LTE TA was issued frequently enough for a positioning application and that the associated error statistics afforded an accurate estimate. Observation of error statistics allowed us to build a realistic LTE TA error model suitable for use in simulation that takes into account channel type. We were also able to validate with field data the analytically derived Gaussian equivalency.

As stated in Chapter 2, most previous TA-based studies in the literature made two critical assumptions about TA behavior: that the additional error introduced by the TA was uniform and that error was independent of the UE location within the TA annulus. Those studies that did use real-world TAs were not focused on evaluating the TA *per se*. Our extensive field experimentation validated the assumption of the uniformity of the error, however, we also showed that the model is better served as normal since the error associated with the

eNB's estimate of the UE distance is dominant relative to the annular rounding in LTE[46]. Furthermore, we validated the second assumption of the independence of the error model with the UE annular offset ψ both through analysis and field experimentation.

Finally, our field experimentation with CeSAR in conjunction with real-world TA values lent validity to the simulated results and showed that an efficient position estimate could be made when CeSAR was leveraged to improve the position estimate. Also notable is that we demonstrated the achievable performance inside a real-world LTE network deployment with entirely empirical data.

9.2 Future Work

This work presented contributions which, when extended, offer the opportunity for further exploration. Specifically, we suggest extension of this work in four areas: three dimensional positioning, uplink observation modeling, heterogeneous network observation, baseband processor performance evaluation, and studying the use of the C-RNTI to best anonymize transmissions.

9.2.1 Positioning in $\mathbb{R}^3$

Here we propose further work which seeks to provide a position estimate in three dimensions. In dense urban environments the UE is not always at ground level due to mobility in skyscrapers, high rises, and other urban clutter. Thus, a TA-based position estimate in $\mathbb{R}^2$ may result in significant error for a UE which is located high above ground level.

Including a CeSAR sensor, particularly at the base of a structure in which a UE may be located, could have two potential benefits which are similar to advantages of CeSAR explored in $\mathbb{R}^2$ in this work. First, and most obvious, is that adding an extra dimension to the position estimate will always improve accuracy (assuming the error associated with that measurement is at least as good as the measurements currently defining the existing system of equations). Second, if a UE is suspected to be in a particular tall structure, placing the CeSAR sensor at the bottom of the structure realizes an approximately orthogonal

[46]This is another intuitive but more general way of stating the necessary conditions for Theorem 1 and QT2 to apply.

measurement relative to the UE-infrastructure geometry. As seen in this work, this will minimize the effects associated with GDoP.

9.2.2 Uplink Frame Observation Modeling

In this work, uplink frame observation was done with a BPSK PN sequence and a matched filter. In a realistic application, the uplink burst will be transmitted after further being OFDM modulated. OFDM transmissions will be more robust in a fading channel and thus have the potential to improve the performance of CeSAR augmentation. Furthermore, the PN sequence used was optimized to improve correlation performance via a LFSR. Real-world LTE frames will not necessarily have these favorable correlation characteristics, thus the resulting correlation will not be as exact.

Specifically, the theory associated with developing an optimal detector of the UE frame (e.g., the Neyman-Pearson detector) would significantly complement the CeSAR method and provide further insight into expected real-world performance. Of particular interest would be leveraging the cyclic prefix and regular signals with specific periodic transmissions such as UE-generated pilot tones to improve detection.

9.2.3 Heterogeneous Network Ecology

At the time of this writing the author is not aware of any fully deployed heterogeneous network in the United States. Therefore, in this work, performance in the presence of physically disparate carrier aggregation was evaluated either entirely in simulation or empirical data were collected from individual eNBs online then combined offline in post processing to mimic a heterogeneous network deployment.

In the near future it is likely that LTE release 11 characteristics will begin to make an entrance in the currently deployed architecture. Studying the behavior of the TA in a real-world heterogeneous implementation would be invaluable. In particular, of interest would be the statistics of TA error associated with SCells, whether those statistics are similar to the PCell statistics, and the use of these errors in case studies to validate performance characteristics.

9.2.4 Effect of the Baseband Processor

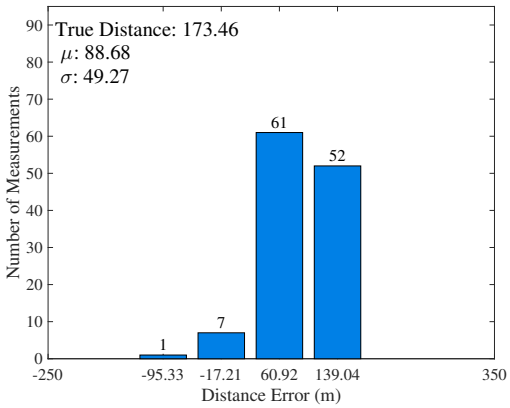
In this study TAs were issued to and observed by two different test phones both operating with the Qualcomm Snapdragon chipset. A comprehensive statistical study of the TA in conjunction with different chipset vendors and versions would be of interest. Among general chipsets available on the market, the Samsung Exynos and Qualcomm Snapdragon are the most pervasive and would provide a starting point in terms of the survey. Within these two chipsets evaluating different versions would also be of interest. Ultimately, building an understanding of how TA-based positioning varies with chipset would be valuable.

9.2.5 Vulnerability in the LTE Software Address Space

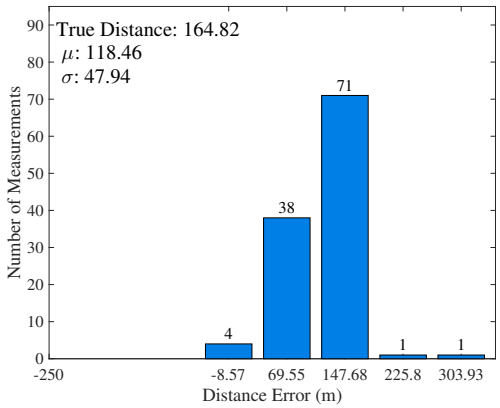
The LTE software address space was presented in this work as a weak component of a LPPM. To this end it serves to anonymize transmissions sent to a specific UE as the C-RNTI stands in as a software address in place of the permanent address (IMSI) assigned to the UE. Evaluating the ability to link a specific user to a C-RNTI would be of particular interest. Methods that could be leveraged may include C-RNTI chaining and deanonymization attacks.

C-RNTI chaining is a method of UE attribution to a C-RNTI that follows that user through initial network negotiation. By observing the initial C-RNTI issuance and then following the user as different C-RNTIs are issued, a valid UE to C-RNTI mapping can theoretically be maintained. As discussed in Chapter 2, several methods have proven effective at linking anonymous data to specific users. Evaluating their efficacy in the LTE software address space would be of interest both in simulation and in real-world network deployments. By evaluating the inherent vulnerability in the C-RNTI anonymization schema, recommendations to improve the method in the context of optimal C-RNTI lease time and initial C-RNTI issuance.

APPENDIX A:
Histograms Representing the Error Associated with TA-Based Distance Estimation

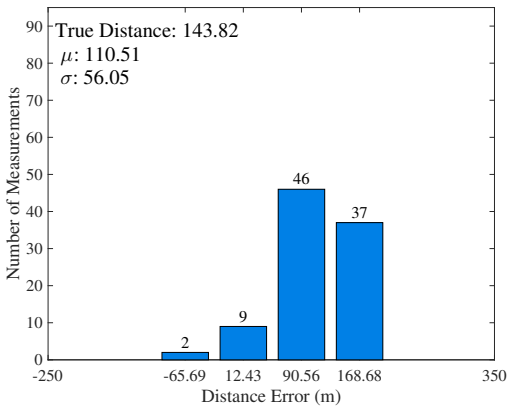


(a) LoS

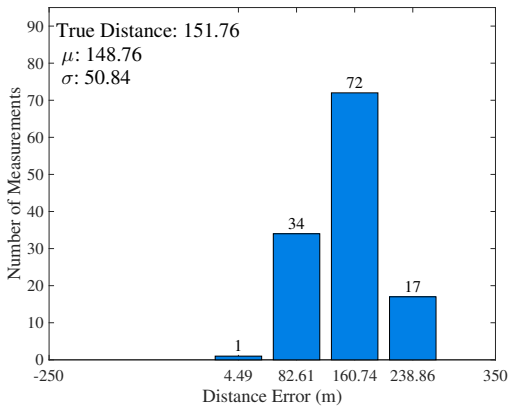


(b) NLoS

Figure A.1. Location A error histograms are presented in this figure. Location A is characterized as a dense urban environment. Adapted from [21].

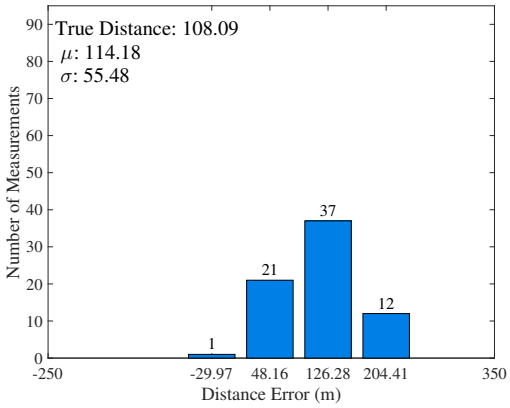


(a) LoS

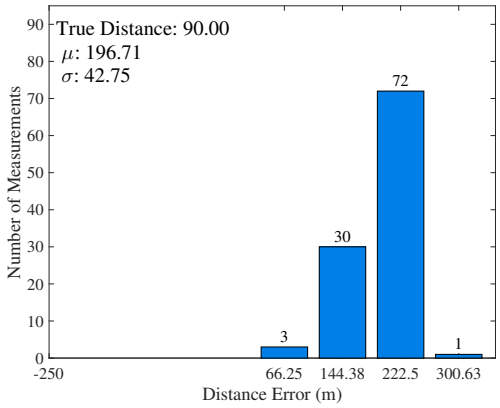


(b) NLoS

Figure A.2. Location B error histograms are presented in this figure. Location B is characterized as a dense urban environment. Adapted from [21].

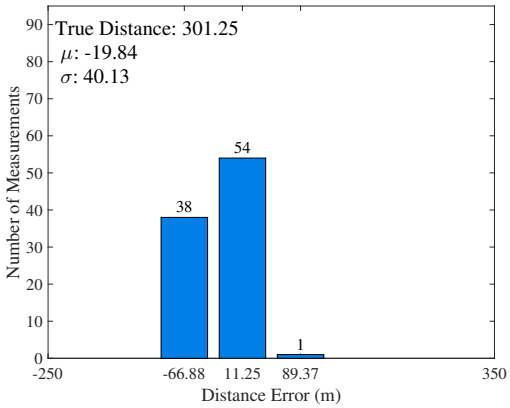


(a) LoS

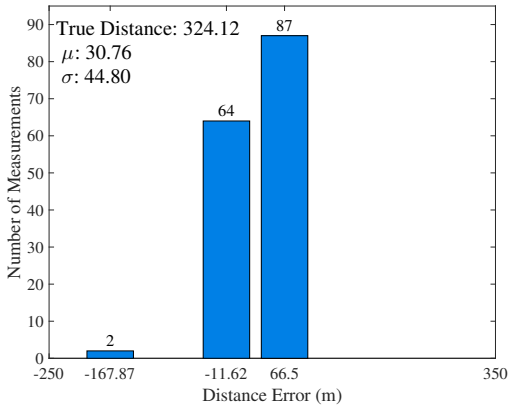


(b) NLoS

Figure A.3. Location C error histograms are presented in this figure. Location B is characterized as a dense urban environment. Adapted from [21].



(a) LoS



(b) NLoS

Figure A.4. Location D error histograms are presented in this figure. Location D is characterized as a suburban environment. Adapted from [21].

APPENDIX B:
Proof of the Lower Bound for an Unbiased Estimator

In this section, we provide the proof of the relationship described by (6.2) and (6.1). The derivation is adapted from [75].

Definition A1: *An admissible estimate is the estimation of a parameter on which observations of a RV depend such that the support of the RV density does not depend on the parameter to be estimated.*

Theorem A1: *Suppose* $\boldsymbol{X} = \{X_1, X_2, \ldots, X_N\}$ *are a set of observations of the RV* x *which is parameterized by* λ and $\tilde{\lambda}(\boldsymbol{X})$ *is an unbiased estimator of* λ*. Then*

$$\mathrm{E}\left\{\left(\tilde{\lambda}(\boldsymbol{X}) - \lambda\right)^2\right\} \geq -\mathrm{E}\left\{\frac{\partial^2 \log \mathrm{p}(\boldsymbol{X}|\lambda)}{\partial \lambda^2}\right\}^{-1} \tag{B.1}$$

if $\tilde{\lambda}(\boldsymbol{X})$ *constitutes an admissible estimate.*

Proof: By definition $\tilde{\lambda}(\boldsymbol{X})$ is an unbiased estimator so the expected value of the estimate is given by

$$\int_a^b \tilde{\lambda}(\boldsymbol{X})\mathrm{p}(\boldsymbol{X}|\lambda)dx = \lambda \tag{B.2}$$

where the limits of the definite integral $[a, b]$ span the support of $\mathrm{p}(\boldsymbol{X}|\lambda)$. Next taking the derivative of both sides w.r.t. λ

$$\frac{\partial}{\partial \lambda}\int_a^b \tilde{\lambda}(\boldsymbol{X})\mathrm{p}(\boldsymbol{X}|\lambda)dx = 1 \tag{B.3}$$

and from Leibniz's rule

$$\int_a^b \frac{\partial}{\partial \lambda}\tilde{\lambda}(\boldsymbol{X})\mathrm{p}(\boldsymbol{X}|\lambda)dx + \frac{\partial b}{\partial \lambda}\tilde{\lambda}(b)\mathrm{p}(b|\lambda) - \frac{\partial a}{\partial \lambda}\tilde{\lambda}(a)\mathrm{p}(a|\lambda) = 1 \tag{B.4}$$

but, by Definition 1, the latter two summands evaluate to zero since

$$\begin{aligned} \frac{\partial a}{\partial \lambda} &= 0 \\ \frac{\partial b}{\partial \lambda} &= 0. \end{aligned} \tag{B.5}$$

Therefore, we have

$$\int \tilde{\lambda}(\boldsymbol{X}) \frac{\partial}{\partial \lambda} \mathrm{p}(\boldsymbol{X}|\lambda) dx = 1 \tag{B.6}$$

where we have dropped the limits of the integral for convenience.

Lemma A1: *For an admissible estimate of the parameter* λ

$$\frac{\partial}{\partial \lambda} \int \mathrm{p}(x|\lambda) dx = \int \frac{\partial}{\partial \lambda} \mathrm{p}(x|\lambda) dx = 0. \tag{B.7}$$

Proof: It follows from Definition 1 and Leibniz's rule that

$$\frac{\partial}{\partial \lambda} \int \mathrm{p}(x|\lambda) dx = \int \frac{\partial}{\partial \lambda} \mathrm{p}(x|\lambda) dx. \tag{B.8}$$

We can then show that

$$\frac{\partial}{\partial \lambda} \int \mathrm{p}(x|\lambda) dx = \frac{\partial}{\partial \lambda} 1 = 0 \tag{B.9}$$

which follows from the definition of a probability density. □

Continuing with the proof of the theorem, we can then let

$$\int \tilde{\lambda}(\boldsymbol{X}) \frac{\partial}{\partial \lambda} \mathrm{p}(\boldsymbol{X}|\lambda) dx - \int \lambda \frac{\partial}{\partial \lambda} \mathrm{p}(\boldsymbol{X}|\lambda) dx = \int \left(\tilde{\lambda}(\boldsymbol{X}) - \lambda \right) \frac{\partial}{\partial \lambda} \mathrm{p}(\boldsymbol{X}|\lambda) dx = 1 \tag{B.10}$$

and

$$\int \left(\tilde{\lambda}(\boldsymbol{X}) - \lambda \right) \frac{1}{\mathrm{p}(\boldsymbol{X}|\lambda)} \frac{\partial}{\partial \lambda} \left(\mathrm{p}(\boldsymbol{X}|\lambda) \right) \mathrm{p}(\boldsymbol{X}|\lambda) dx = 1. \tag{B.11}$$

Now substituting the relationship

$$\frac{\partial}{\partial \lambda} \log \mathrm{p}(\boldsymbol{X}|\lambda) = \frac{1}{\mathrm{p}(\boldsymbol{X}|\lambda)} \frac{\partial}{\partial \lambda} \mathrm{p}(\boldsymbol{X}|\lambda) \tag{B.12}$$

we have that

$$\int \left(\tilde{\lambda}(\boldsymbol{X}) - \lambda\right) \frac{\partial}{\partial \lambda} \left(\log \mathrm{p}(\boldsymbol{X}|\lambda)\right) \mathrm{p}(\boldsymbol{X}|\lambda) dx = 1. \tag{B.13}$$

Using the definition of expectation the relationship becomes

$$\mathrm{E}\left\{\left(\tilde{\lambda}(\boldsymbol{X}) - \lambda\right) \frac{\partial}{\partial \lambda} \left(\log \mathrm{p}(\boldsymbol{X}|\lambda)\right)\right\} = 1. \tag{B.14}$$

The Cauchy-Schwarz inequality[47] then gives

$$\mathrm{E}\left\{\left(\tilde{\lambda}(\boldsymbol{X}) - \lambda\right)^2\right\} \mathrm{E}\left\{\left(\frac{\partial}{\partial \lambda} \log \mathrm{p}(\boldsymbol{X}|\lambda)\right)^2\right\} \geq \left|\mathrm{E}\left\{\left(\tilde{\lambda}(\boldsymbol{X}) - \lambda\right) \frac{\partial}{\partial \lambda} \left(\log \mathrm{p}(\boldsymbol{X}|\lambda)\right)\right\}\right|^2 = 1 \tag{B.15}$$

$$\mathrm{E}\left\{\left(\tilde{\lambda}(\boldsymbol{X}) - \lambda\right)^2\right\} \mathrm{E}\left\{\left(\frac{\partial}{\partial \lambda} \log \mathrm{p}(\boldsymbol{X}|\lambda)\right)^2\right\} \geq 1. \tag{B.16}$$

$$\mathrm{E}\left\{\left(\tilde{\lambda}(\boldsymbol{X}) - \lambda\right)^2\right\} \geq \mathrm{E}\left\{\left(\frac{\partial}{\partial \lambda} \log \mathrm{p}(\boldsymbol{X}|\lambda)\right)^2\right\}^{-1}. \tag{B.17}$$

Lemma A2: *For an admissible estimate of the parameter* λ

$$\mathrm{E}\left\{\left(\frac{\partial}{\partial \lambda} \log \mathrm{p}(\boldsymbol{X}|\lambda)\right)^2\right\} = -\mathrm{E}\left\{\frac{\partial^2}{\partial \lambda^2} \log \mathrm{p}(\boldsymbol{X}|\lambda)\right\}. \tag{B.18}$$

Proof: From the property of a probability density we have

$$\int \mathrm{p}(\boldsymbol{X}|\lambda) dx = 1. \tag{B.19}$$

Now differentiating both sides of the relationship

$$\frac{\partial}{\partial \lambda} \int \mathrm{p}(\boldsymbol{X}|\lambda) dx = 0. \tag{B.20}$$

Again, invoking Definition 1 and Leibniz's rule the relationship becomes

$$\frac{\partial}{\partial \lambda} \int \mathrm{p}(\boldsymbol{X}|\lambda) dx = \int \frac{\partial}{\partial \lambda} \mathrm{p}(\boldsymbol{X}|\lambda) dx = 0. \tag{B.21}$$

[47] $\mathrm{E}\{U^2\}\mathrm{E}\{V^2\} \geq |\mathrm{E}\{UV\}|^2$ [48].

We now use the relationship (B.12) to write

$$\int \frac{\partial \log \mathrm{p}(\boldsymbol{X}|\lambda)}{\partial \lambda} \mathrm{p}(\boldsymbol{X}|\lambda) dx = 0 \tag{B.22}$$

and again differentiate both sides of the equation to realize

$$\frac{\partial}{\partial \lambda} \int \frac{\partial \log \mathrm{p}(\boldsymbol{X}|\lambda)}{\partial \lambda} \mathrm{p}(\boldsymbol{X}|\lambda) dx = \int \frac{\partial}{\partial \lambda} \left(\frac{\partial \log \mathrm{p}(\boldsymbol{X}|\lambda)}{\partial \lambda} \mathrm{p}(\boldsymbol{X}|\lambda) \right) dx = 0 \tag{B.23}$$

which is again possible from Definition 1 and Leibniz's rule. The chain rule then gives

$$\int \frac{\partial^2 \log \mathrm{p}(\boldsymbol{X}|\lambda)}{\partial \lambda^2} \mathrm{p}(\boldsymbol{X}|\lambda) dx + \int \frac{\partial \log \mathrm{p}(\boldsymbol{X}|\lambda)}{\partial \lambda} \frac{\partial \mathrm{p}(\boldsymbol{X}|\lambda)}{\partial \lambda} dx = 0. \tag{B.24}$$

The relationship in (B.12) is the substituted into the second summand to realize

$$\int \frac{\partial^2 \log \mathrm{p}(\boldsymbol{X}|\lambda)}{\partial \lambda^2} \mathrm{p}(\boldsymbol{X}|\lambda) dx + \int \frac{\partial \log \mathrm{p}(\boldsymbol{X}|\lambda)}{\partial \lambda} \frac{\partial \log \mathrm{p}(\boldsymbol{X}|\lambda)}{\partial \lambda} \mathrm{p}(\boldsymbol{X}|\lambda) dx = 0 \tag{B.25}$$

$$\int \frac{\partial^2 \log \mathrm{p}(\boldsymbol{X}|\lambda)}{\partial \lambda^2} \mathrm{p}(\boldsymbol{X}|\lambda) dx + \int \left(\frac{\partial \log \mathrm{p}(\boldsymbol{X}|\lambda)}{\partial \lambda} \right)^2 \mathrm{p}(\boldsymbol{X}|\lambda) dx = 0 \tag{B.26}$$

$$\int \left(\frac{\partial \log \mathrm{p}(\boldsymbol{X}|\lambda)}{\partial \lambda} \right)^2 \mathrm{p}(\boldsymbol{X}|\lambda) dx = - \int \frac{\partial^2 \log \mathrm{p}(\boldsymbol{X}|\lambda)}{\partial \lambda^2} \mathrm{p}(\boldsymbol{X}|\lambda) dx \tag{B.27}$$

$$\mathrm{E}\left\{ \left(\frac{\partial \log \mathrm{p}(\boldsymbol{X}|\lambda)}{\partial \lambda} \right)^2 \right\} = -\mathrm{E}\left\{ \frac{\partial^2 \log \mathrm{p}(\boldsymbol{X}|\lambda)}{\partial \lambda^2} \right\}. \quad \square \tag{B.28}$$

To finish the proof of the theorem we use the result of Lemma A2 in (B.17) to arrive at

$$\mathrm{E}\left\{ \left(\tilde{\lambda}(\boldsymbol{X}) - \lambda \right)^2 \right\} \geq -\mathrm{E}\left\{ \frac{\partial^2 \log \mathrm{p}(\boldsymbol{X}|\lambda)}{\partial \lambda^2} \right\}^{-1}. \quad \blacksquare \tag{B.29}$$

APPENDIX C:
Proof of the Maximum Likelihood Estimate and the Cramér-Rao Lower Bound for Source Localization with Normally Corrupted Measurements

Theorem A2: *The maximum likelihood estimate (MLE) for source localization with normally corrupted measurements is given by*

$$\begin{aligned} \sum_{i=1}^{N} \frac{(d_i - \hat{d}_i)(x_0 - x_i)}{d_i} &= 0 \\ \sum_{i=1}^{N} \frac{(d_i - \hat{d}_i)(y_0 - y_i)}{d_i} &= 0 \end{aligned} \tag{C.1}$$

when $\sigma_i = \sigma, \forall i$ *and the source position is* $\mathbf{p_0} = [x_0, y_0]^T$.

Proof: Since the measurements $\hat{\boldsymbol{d}}$ are corrupted by Gaussian noise we can define the joint error distribution as

$$\mathrm{p}(\hat{\boldsymbol{d}}|\boldsymbol{d}) = \prod_{i=1}^{N} \frac{1}{\sqrt{2\pi}\sigma_i} e^{\frac{-(\hat{d}_i - d_i)^2}{2\sigma_i^2}}. \tag{C.2}$$

The resulting log-likelihood function is given by

$$\log \mathrm{p}(\hat{\boldsymbol{d}}|\boldsymbol{d}) = \sum_{i=1}^{N} -\log(\sqrt{2\pi}\sigma_i) + \frac{-(\hat{d}_i - d_i)^2}{2\sigma_i^2}. \tag{C.3}$$

When we let $\sigma_i = \sigma, \forall i$ the log-likelihood function is simplified to

$$\log \mathrm{p}(\hat{\boldsymbol{d}}|\boldsymbol{d}) = NC + \sum_{i=1}^{N} \frac{-(\hat{d}_i - d_i)^2}{2\sigma^2}. \tag{C.4}$$

where $C = -\log(\sqrt{2\pi}\sigma)$ is a constant. The MLE $\hat{\mathbf{p}}$ will then be the location $\mathbf{p} = [x, y]^T$

that maximizes $\log \mathrm{p}(\hat{\boldsymbol{d}}|\boldsymbol{d})$ such that

$$\hat{\mathbf{p}} = \arg\max_{\mathbf{p}} \log \mathrm{p}(\hat{\boldsymbol{d}}|\boldsymbol{d}). \tag{C.5}$$

The maxima of (C.5) can then be found by setting the first derivative equal to zero and solving for $\mathbf{p}$.

Lemma A3: *The partial derivative of the distance, d, with respect to* $\mathbf{p}$ *is*

$$\frac{\partial}{\partial x} d_i = \frac{(x - x_i)}{d_i} \tag{C.6}$$

and

$$\frac{\partial}{\partial y} d_i = \frac{(y - y_i)}{d_i}. \tag{C.7}$$

Proof: Let

$$\begin{aligned} d_i &= \| \mathbf{p} - \mathbf{p}_i \| \\ &= \sqrt{(x - x_i)^2 + (y - y_i)^2} \end{aligned} \tag{C.8}$$

then by the chain rule

$$\begin{aligned} \frac{\partial}{\partial x} d_i &= \frac{2(x - x_i)}{2\sqrt{(x - x_i)^2 + (y - y_i)^2}} \\ &= \frac{(x - x_i)}{d_i}. \end{aligned} \tag{C.9}$$

The partial derivative with respect to y follows from the same methodology. □

Now, continuing with the proof of Theorem A2, consider the partial derivative of (C.4) with respect to x

$$\begin{aligned} \frac{\partial}{\partial x} \log \mathrm{p}(\hat{\boldsymbol{d}}|\boldsymbol{d}) &= \frac{\partial}{\partial x} NC + \sum_{i=1}^{N} \frac{\partial}{\partial x} \frac{-(\hat{d}_i - d_i)^2}{2\sigma^2} \\ &= \sum_{i=1}^{N} \frac{2(\hat{d}_i - d_i)}{2\sigma^2} \frac{\partial}{\partial x} d_i \end{aligned} \tag{C.10}$$

which follows from the chain rule and from the fact that the derivative of a constant is zero.

Then invoking Lemma A3 we have that

$$\frac{\partial}{\partial x}\log \mathrm{p}(\hat{\boldsymbol{d}}|\boldsymbol{d}) = \sum_{i=1}^{N} \frac{(\hat{d}_i - d_i)(x - x_i)}{\sigma^2 d_i}. \tag{C.11}$$

The first partial derivative with respect to y can be found by analogous means. The relationship in (C.11) can be further simplified when finding the maxima of (C.5) by ignoring the constant σ^{-2} (assuming the condition $\sigma_i = \sigma, \forall i$). ■

Theorem A3: *The Cramér-Rao Lower Bound for unbiased position estimation is given by*

$$\mathrm{CRLB} = \sqrt{\mathrm{tr}(\mathbf{I}^{-1})} \tag{C.12}$$

and

$$\mathbf{I}_{\{i,j\}} = -\mathrm{E}\left\{\frac{\partial^2 \log \mathrm{p}(\hat{\boldsymbol{d}}|\boldsymbol{d})}{\partial \mathbf{p}_{\{i\}} \partial \mathbf{p}_{\{j\}}}\right\} \tag{C.13}$$

where

$$\mathbf{I} = \begin{bmatrix} \sum_{i=1}^{N} \frac{(x-x_i)^2}{\sigma^2 d_i^2} & \sum_{i=1}^{N} \frac{(x-x_i)(y-y_i)}{\sigma^2 d_i^2} \\ \sum_{i=1}^{N} \frac{(x-x_i)(y-y_i)}{\sigma^2 d_i^2} & \sum_{i=1}^{N} \frac{(y-y_i)^2}{\sigma^2 d_i^2} \end{bmatrix}. \tag{C.14}$$

when the distance measurements, $\hat{d}_i$, are corrupted by Gaussian noise and $\sigma_i = \sigma, \forall i$.

Proof: Consider

$$\mathbf{I}_{\{1,1\}} = -\mathrm{E}\left\{\frac{\partial^2}{\partial x^2}\log \mathrm{p}(\hat{\boldsymbol{d}}|\boldsymbol{d})\right\} \tag{C.15}$$

where $\mathbf{p} = [x, y]^T$ so $\mathbf{p}_{\{1\}} = x$ and $\mathbf{p}_{\{2\}} = y$. The relationship in (C.15) can then be expanded to

$$\begin{aligned} \mathbf{I}_{\{1,1\}} &= -\mathrm{E}\left\{\frac{\partial}{\partial x}\frac{\partial}{\partial x}\log \mathrm{p}(\hat{\boldsymbol{d}}|\boldsymbol{d})\right\} \\ &= -\mathrm{E}\left\{\frac{\partial}{\partial x}\frac{1}{\sigma^2}\sum_{i=1}^{N}\frac{(\hat{d}_i - d_i)(x - x_i)}{d_i}\right\} \end{aligned} \tag{C.16}$$

which follows from Theorem A2. Now, again evaluating the partial derivative we have

$$\begin{aligned}\frac{\partial}{\partial x}\frac{1}{\sigma^2}\sum_{i=1}^{N}\frac{(\hat{d}_i - d_i)(x - x_i)}{d_i} &= \frac{1}{\sigma^2}\sum_{i=1}^{N}\frac{\partial}{\partial x}\frac{(\hat{d}_i - d_i)(x - x_i)}{d_i} \\ &= \frac{1}{\sigma^2}\sum_{i=1}^{N}\frac{\partial}{\partial x}\left((\hat{d}_i - d_i)\frac{\partial}{\partial x}d_i\right) \\ &= \frac{1}{\sigma^2}\sum_{i=1}^{N}\frac{\partial}{\partial x}(\hat{d}_i - d_i)\frac{\partial}{\partial x}d_i + (\hat{d}_i - d_i)\frac{\partial^2}{\partial x^2}d_i \\ &= \frac{1}{\sigma^2}\sum_{i=1}^{N}(\hat{d}_i - d_i)\frac{\partial^2}{\partial x^2}d_i - \left(\frac{\partial}{\partial x}d_i\right)^2\end{aligned} \tag{C.17}$$

which follows from the product rule. Now substituting back into (C.16) we have

$$\begin{aligned}-\mathrm{E}\left\{\frac{\partial}{\partial x}\frac{1}{\sigma^2}\sum_{i=1}^{N}\frac{(\hat{d}_i - d_i)(x - x_i)}{d_i}\right\} &= \frac{-1}{\sigma^2}\sum_{i=1}^{N}\mathrm{E}_{\hat{d}}\left\{(\hat{d}_i - d_i)\frac{\partial^2}{\partial x^2}d_i\right\} - \mathrm{E}_{\hat{d}}\left\{\left(\frac{\partial}{\partial x}d_i\right)^2\right\} \\ &= \frac{1}{\sigma^2}\sum_{i=1}^{N}\left(\frac{\partial}{\partial x}d_i\right)^2\end{aligned} \tag{C.18}$$

which follows from the following two relationships when the expectation is taken with respect to the RV $\hat{d}$

$$\begin{aligned}\mathrm{E}_{\hat{d}}\left\{\left(\frac{\partial}{\partial x}d_i\right)^2\right\} &= \left(\frac{\partial}{\partial x}d_i\right)^2 \\ \mathrm{E}_{\hat{d}}\left\{(\hat{d}_i - d_i)\frac{\partial^2}{\partial x^2}d_i\right\} &= 0.\end{aligned} \tag{C.19}$$

The former relationship is clear since the expectation is take over a constant relative to $\hat{d}$. The latter relationship follows from the fact that $\mathrm{E}_{\hat{d}}\left\{\hat{d}_i - d_i\right\} = 0$ if the estimate is unbiased.

Finally, we use the result of Lemma A3 to expand (C.18) to

$$\begin{aligned}\mathbf{I}_{\{1,1\}} &= \frac{1}{\sigma^2}\sum_{i=1}^{N}\left(\frac{\partial}{\partial x}d_i\right)^2 \\ &= \frac{1}{\sigma^2}\sum_{i=1}^{N}\left(\frac{(x-x_i)}{d_i}\right)^2 \\ &= \frac{1}{\sigma^2}\sum_{i=1}^{N}\frac{(x-x_i)^2}{d_i^2}.\end{aligned} \tag{C.20}$$

This result can be easily extended by Lemma A3 to show

$$\mathbf{I}_{\{2,2\}} = \frac{1}{\sigma^2}\sum_{i=1}^{N}\frac{(y-y_i)^2}{d_i^2}. \tag{C.21}$$

The off-diagonal elements of $\mathbf{I}$ can be found by replacing the second derivative in (C.16) with

$$\mathbf{I}_{\{1,2\}} = -\mathrm{E}\left\{\frac{\partial}{\partial y}\frac{1}{\sigma^2}\sum_{i=1}^{N}\frac{(\hat{d}_i - d_i)(x-x_i)}{d_i}\right\}. \tag{C.22}$$

Evaluating the partial derivative with respect to y we have

$$\begin{aligned}\frac{\partial}{\partial y}\frac{1}{\sigma^2}\sum_{i=1}^{N}\frac{(\hat{d}_i - d_i)(x-x_i)}{d_i} &= \frac{1}{\sigma^2}\sum_{i=1}^{N}\frac{\partial}{\partial y}\frac{(\hat{d}_i - d_i)(x-x_i)}{d_i} \\ &= \frac{1}{\sigma^2}\sum_{i=1}^{N}\frac{\partial}{\partial y}\left((\hat{d}_i - d_i)\frac{\partial}{\partial x}d_i\right) \\ &= \frac{1}{\sigma^2}\sum_{i=1}^{N}\frac{\partial}{\partial y}(\hat{d}_i - d_i)\frac{\partial}{\partial x}d_i + (\hat{d}_i - d_i)\frac{\partial}{\partial y}\frac{\partial}{\partial x}d_i \\ &= \frac{1}{\sigma^2}\sum_{i=1}^{N}(\hat{d}_i - d_i)\frac{\partial}{\partial y}\frac{\partial}{\partial x}d_i - \left(\frac{\partial}{\partial y}d_i\right)\left(\frac{\partial}{\partial x}d_i\right).\end{aligned} \tag{C.23}$$

Then, substituting this result into (C.22) we have

$$-\mathrm{E}\left\{\frac{\partial}{\partial y}\frac{1}{\sigma^2}\sum_{i=1}^{N}\frac{(\hat{d}_i - d_i)(x - x_i)}{d_i}\right\} = \frac{-1}{\sigma^2}\sum_{i=1}^{N}\mathrm{E}_{\hat{d}}\left\{(\hat{d}_i - d_i)\frac{\partial}{\partial y}\frac{\partial}{\partial x}d_i\right\} - \mathrm{E}_{\hat{d}}\left\{\left(\frac{\partial}{\partial y}d_i\right)\left(\frac{\partial}{\partial x}d_i\right)\right\}$$
$$= \frac{1}{\sigma^2}\sum_{i=1}^{N}\left(\frac{\partial}{\partial y}d_i\right)\left(\frac{\partial}{\partial x}d_i\right) \tag{C.24}$$

where the last step follows from the results enumerated in (C.19). Finally, using the results of Lemma A3 we have

$$\frac{1}{\sigma^2}\sum_{i=1}^{N}\left(\frac{\partial}{\partial y}d_i\right)\left(\frac{\partial}{\partial x}d_i\right) = \frac{1}{\sigma^2}\sum_{i=1}^{N}\frac{(x - x_i)(y - y_i)}{d_i^2}. \tag{C.25}$$

Note that the matrix $\mathbf{I}$ will be symmetric, therefore, $\mathbf{I}_{\{1,2\}} = \mathbf{I}_{\{2,1\}}$. ■

APPENDIX D: Derivation of the Maximum Likelihood Estimate Associated with $p_{\mathcal{N}}(x) * p_U(x)$

In this section, a derivation of the convolution $p_{\mathcal{N}}(x) * p_U(x)$ is given. To begin, recall

$$p_{\mathcal{N}}(x) = \frac{1}{\sqrt{2\pi}\sigma} e^{\frac{-(x)^2}{2\sigma^2}} = \mathcal{N}(0, \sigma^2) \tag{D.1}$$

and

$$p_U(x) = \frac{1}{\tau}\mathbf{I}_{[-\tau/2,\tau/2]}(x) \tag{D.2}$$

where $\mathbf{I}_{[-\tau/2,\tau/2]}(\cdot)$ is the indicator function with support $\in [-\tau/2, \tau/2]$.

Next, using t as the dummy variable for the convolution we have

$$p_{\mathcal{N}}(x) * p_U(x) = \frac{1}{\tau}\int_{x-\tau/2}^{x+\tau/2} \frac{1}{\sqrt{2\pi}\sigma} e^{\frac{-(t)^2}{2\sigma^2}} dt. \tag{D.3}$$

Evaluating the integral we have

$$\begin{aligned} \frac{1}{\tau}\int_{x-\tau/2}^{x+\tau/2} \frac{1}{\sqrt{2\pi}\sigma} e^{\frac{-(t)^2}{2\sigma^2}} dt &= \frac{1}{\tau}\,\Phi\left(\frac{t}{\sigma}\right)\Big|_{x-\tau/2}^{x+\tau/2} \\ &= \frac{1}{\tau}\left(\Phi\left(\frac{x+\tau/2}{\sigma}\right) - \Phi\left(\frac{x-\tau/2}{\sigma}\right)\right) \end{aligned} \tag{D.4}$$

where

$$\Phi\left(\frac{x-\mu}{\sigma}\right) \tag{D.5}$$

is the cumulative density of $\mathcal{N}(\mu, \sigma^2)$.

Next, to find the maximum-likelihood estimate (MLE) of $p_{\mathcal{N}}(x) * p_U(x)$ for positioning applications consider

$$\hat{\mathbf{p}} = \arg\max_{\mathbf{p}} \log \mathrm{p}(\hat{\boldsymbol{d}}|\boldsymbol{d}) \tag{D.6}$$

where

$$\log \mathrm{p}(\hat{\boldsymbol{d}}|\boldsymbol{d}) = \sum_{i=1}^{N} \log \mathrm{p}(\hat{d}_i|d_i). \tag{D.7}$$

and $\boldsymbol{d} = [d_1, d_2, \ldots, d_N]^T$ is the set of actual distances to the N eNBs, $\hat{\boldsymbol{d}} = [\hat{d}_1, \hat{d}_2, \ldots, \hat{d}_N]^T$ is the set of measured distances to the N eNBs. The above density given in (D.4) can be reformulated for the positioning problem with non-zero mean as

$$\mathrm{p}(\hat{d}_i|d_i) = \frac{1}{\tau}\left(\Phi\left(\frac{\hat{d}_i - d_i - \tau/2}{\sigma_i}\right) - \Phi\left(\frac{\hat{d}_i - d_i + \tau/2}{\sigma_i}\right)\right). \tag{D.8}$$

The corresponding MLE can then be found as

$$\begin{aligned}
&\frac{\partial \log \mathrm{p}(\hat{\boldsymbol{d}}|\boldsymbol{d})}{\partial x} = \\
&\frac{1}{\tau}\sum_{i=1}^{N} \mathcal{F}^{-1}(d_i)\left(\mathcal{N}(\hat{d}_i - d_i - \tau/2, \sigma^2)\frac{\partial}{\partial x}d_i\right. \\
&\qquad\qquad \left. -\mathcal{N}(\hat{d}_i - d_i + \tau/2, \sigma^2)\frac{\partial}{\partial x}d_i\right) \\
&\frac{\partial \log \mathrm{p}(\hat{\boldsymbol{d}}|\boldsymbol{d})}{\partial y} = \\
&\frac{1}{\tau}\sum_{i=1}^{N} \mathcal{F}^{-1}(d_i)\left(\mathcal{N}(\hat{d}_i - d_i - \tau/2, \sigma^2)\frac{\partial}{\partial y}d_i\right. \\
&\qquad\qquad \left. -\mathcal{N}(\hat{d}_i - d_i + \tau/2, \sigma^2)\frac{\partial}{\partial y}d_i\right)
\end{aligned} \tag{D.9}$$

where we have assumed for simplicity that $\sigma_i = \sigma \; \forall i$, and

$$\mathcal{F}(d_i) = \Phi\left(\frac{\hat{d}_i - d_i - \tau/2}{\sigma}\right) - \Phi\left(\frac{\hat{d}_i - d_i + \tau/2}{\sigma}\right) \tag{D.10}$$

Then continuing the differentiation and invoking Lemma A3 we have that

$$\begin{aligned}
&\frac{\partial \log \mathrm{p}(\hat{\boldsymbol{d}}|\boldsymbol{d})}{\partial x} = \\
&\frac{1}{\tau}\sum_{i=1}^{N} \mathcal{F}^{-1}(d_i)\frac{(x-x_i)}{d_i}\Big(\mathcal{N}(\mu_i + \hat{d}_i - \tau/2, \sigma^2) \\
&\qquad\qquad -\mathcal{N}(\mu_i + \hat{d}_i + \tau/2, \sigma^2)\Big) \\
&\frac{\partial \log \mathrm{p}(\hat{\boldsymbol{d}}|\boldsymbol{d})}{\partial y} = \\
&\frac{1}{\tau}\sum_{i=1}^{N} \mathcal{F}^{-1}(d_i)\frac{(y-y_i)}{d_i}\Big(\mathcal{N}(\mu_i + \hat{d}_i - \tau/2, \sigma^2) \\
&\qquad\qquad -\mathcal{N}(\mu_i + \hat{d}_i + \tau/2, \sigma^2)\Big).
\end{aligned} \tag{D.11}$$

Setting these gradients to zeros yields the exact MLE $\hat{\mathbf{p}}$ for an error characterized by $p_{\mathcal{N}}(x) * p_U(x)$. ■

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX E:
Proof of the Variance of $\mathcal{N}'$ at Extrema of τ

Theorem A4:

$$\lim_{\tau \to 0} \text{var}\{\mathcal{N}'\}\Big|_{\forall \psi} = \sigma^2_{\mathcal{N}} \tag{E.1}$$

where $\sigma^2_{\mathcal{N}}$ *is the variance of the latent RV.*

Proof: Recall that

$$\text{E}\{\mathcal{N}'^k\} = \frac{1}{j^k} \frac{d^k P_{\mathcal{N}'}(\phi)}{d\phi^k}\bigg|_{\phi=0} \tag{E.2}$$

where $P_{\mathcal{N}'}(\phi)$ is the characteristic function (CF) of $\mathcal{N}'$ [49]. Therefore, the second moment is explicitly given by

$$\text{E}\{\mathcal{N}'^2\} = -\frac{d^2 P_{\mathcal{N}'}(\phi)}{d\phi^2}\bigg|_{\phi=0} \tag{E.3}$$

since $j^{-2} = -1$. Recall also that

$$P_{\mathcal{N}'}(\phi) = \sum_n A_n(\phi - 2\pi n/\tau). \tag{E.4}$$

Lemma A4: *If* U *is uniform then its CF is given by*

$$P_U(\phi) = \text{sinc}\left(\frac{\phi\tau}{2}\right). \tag{E.5}$$

Proof: Note that if $U \sim \frac{1}{\tau} I_{[-\tau/2,\tau/2]}(x)$ then

$$\begin{aligned} P_U(\phi) &= \frac{1}{\tau}\int_{-\tau/2}^{\tau/2} e^{-j\phi x} dx \\ &= -\frac{1}{j\phi\tau} e^{-j\phi x}\Big|_{x=-\tau/2}^{x=\tau/2} \\ &= -\frac{1}{j\phi\tau}\left(e^{\frac{-j\phi\tau}{2}} - e^{\frac{j\phi\tau}{2}}\right) \end{aligned} \tag{E.6}$$

$$
\begin{aligned}
&= \frac{2\sin(\phi\tau/2)}{\phi\tau} \\
&= \frac{\sin(\phi\tau/2)}{\phi\tau/2} \\
&= \operatorname{sinc}\left(\frac{\phi\tau}{2}\right)
\end{aligned} \tag{E.7}
$$

where the last step follows from the definition $\operatorname{sinc}(x) = \sin(x)/x$ and thus implies zero crossings at $\phi = 2\pi k/\tau$ where $k \in \mathbb{Z}$. Note also that $P_U(0) = 1$ which satisfies the requirement that $\int_x \mathrm{p}_U(x)dx = 1$. $\square$

Lemma A5: *If $\mathcal{N}$ is normal then its CF is given by*

$$
P_{\mathcal{N}}(\phi) = e^{\frac{-(\phi\sigma)^2}{2}}. \tag{E.8}
$$

Proof: Note that if $\mathcal{N} \sim \mathcal{N}(0, \sigma^2)$ then

$$
\begin{aligned}
P_{\mathcal{N}}(\phi) &= \int_{-\infty}^{\infty} \frac{1}{\sigma\sqrt{2\pi}} e^{\frac{-x^2}{2\sigma^2}} e^{-j\phi x} dx \\
&= \int_{-\infty}^{\infty} \frac{1}{\sigma\sqrt{2\pi}} e^{\frac{-x^2}{2\sigma^2}} cos(\phi x) dx \\
&= e^{\frac{-(\phi\sigma)^2}{2}}.
\end{aligned} \tag{E.9}
$$

The second step of (E.9) follows from

$$
\int_{-a}^{a} e^{-jx} dx = \int_{-a}^{a} \cos(x)dx + j\int_{-a}^{a} \sin(x)dx = \int_{-a}^{a} \cos(x)dx \tag{E.10}
$$

and the last step in (E.9) is given by Abramowitz and Stegun [76]. Note also that $P_{\mathcal{N}}(0) = 1$ which satisfies the requirement that $\int_x \mathrm{p}_{\mathcal{N}}(x)dx = 1$. $\square$

Next, continuing with the proof of Theorem A4, let $\tau \to 0$ so that $P_{\mathcal{N}'}(\phi) \approx A(\phi) = P_U(\phi)P_{\mathcal{N}}(\phi)$ (cf. Chapter 6). Now to calculate the second moment, by (E.3), Lemmas A4 and A5, and the product rule, we have

$$
-\frac{d^2}{d\phi^2} P_U(\phi)P_{\mathcal{N}}(\phi) = -\frac{d}{d\phi}\left(\operatorname{sinc}\left(\frac{\phi\tau}{2}\right)\frac{d}{d\phi}\left(e^{\frac{-(\phi\sigma)^2}{2}}\right) + \frac{d}{d\phi}\left(\operatorname{sinc}\left(\frac{\phi\tau}{2}\right)\right)e^{\frac{-(\phi\sigma)^2}{2}}\right). \tag{E.11}
$$

And again we invoke the product rule to find that

$$
\begin{aligned}
-\frac{d^2}{d\phi^2} P_U(\phi) P_{\mathcal{N}}(\phi) = & \\
& - \operatorname{sinc}\left(\frac{\phi\tau}{2}\right) \frac{d^2}{d\phi^2}\left(e^{\frac{-(\phi\sigma)^2}{2}}\right) - \frac{d^2}{d\phi^2}\left(\operatorname{sinc}\left(\frac{\phi\tau}{2}\right)\right) e^{\frac{-(\phi\sigma)^2}{2}} \\
& - 2\frac{d}{d\phi}\left(\operatorname{sinc}\left(\frac{\phi\tau}{2}\right)\right) \frac{d}{d\phi}\left(e^{\frac{-(\phi\sigma)^2}{2}}\right).
\end{aligned} \tag{E.12}
$$

Now evaluating individual elements of (E.12) at $\phi = 0$, we have that

$$
\begin{aligned}
\frac{d}{d\phi} e^{\frac{-(\phi\sigma)^2}{2}}\bigg|_{\phi=0} &= 0 \\
\frac{d}{d\phi} \operatorname{sinc}\left(\frac{\phi\tau}{2}\right)\bigg|_{\phi=0} &= 0 \\
\frac{d^2}{d\phi^2} e^{\frac{-(\phi\sigma)^2}{2}}\bigg|_{\phi=0} &= -\sigma^2 \\
\frac{d^2}{d\phi^2} \operatorname{sinc}\left(\frac{\phi\tau}{2}\right)\bigg|_{\phi=0} &= \frac{-\tau^2}{12}
\end{aligned} \tag{E.13}
$$

where the first three relationships follow directly and the last follows from the variance of a uniform random variable. Using these results (E.12) can be simplified to

$$
-\frac{d^2}{d\phi^2} P_U(\phi) P_{\mathcal{N}}(\phi) = \sigma^2 + \frac{\tau^2}{12}. \tag{E.14}
$$

Finally, it is straightforward to verify that

$$
\lim_{\tau \to 0} \sigma^2 + \frac{\tau^2}{12} = \sigma^2. \tag{E.15}
$$

Note that the assumption that used to arrive at (E.14) was that $P_{\mathcal{N}'}(\phi) \approx A(\phi)$ which requires that $\tau \leq \epsilon$ where ϵ is some sufficiently small number (cf. Chapter 6). ■

Theorem A5:

$$
\lim_{\tau \to \infty} \operatorname{var}\{\mathcal{N}'\}\Big|_{\psi=0} = 0 \tag{E.16}
$$

and

$$\lim_{\tau\to\infty} \text{var}\{\mathcal{N}'\}\Big|_{\psi=\tau/2} = \infty. \tag{E.17}$$

Proof: Consider the case where $\tau \to \infty$ and recall that $p_{\mathcal{N}'}(x) = \delta(x)$ if there is no annular offset ψ in the sampling function such that $\text{Ш}_\tau(x)$ (cf. Chapter 6). It then follows from the definition of the Fourier transform that

$$P_{\mathcal{N}'}(\phi) = \int_{-\infty}^{\infty} \delta(x) e^{-j\phi x} dx = 1. \tag{E.18}$$

It is also easy to verify that

$$\lim_{\tau\to\infty} \text{var}\{\mathcal{N}'\} = \frac{d^2}{d\phi^2} 1\Big|_{\phi=0} = 0. \tag{E.19}$$

Lemma A6: *If the annular offset is $\psi = \tau/2$ then*

$$p_{\mathcal{N}'}(x) = \frac{1}{2}\delta(x + \tau/2) + \frac{1}{2}\delta(x - \tau/2) \tag{E.20}$$

when $\tau \to \infty$.

Proof: Let the impulsion train be $\text{Ш}_\tau(x - \tau/2)$ so that the annular offset is $\psi = \tau/2$ which is the worst case ψ in terms of the resulting variance of $\mathcal{N}'$ when $\tau \to \infty$. The resulting shifted version of $p_{\mathcal{N}'}(x)$ can then be approximated as (E.20) for sufficiently large τ.

To see this recall that $p_{\mathcal{N}'}(\eta) = \sum_n \alpha\delta(x - n\tau)$ and consider summands where $n \neq 0, 1$. Recall that when the annular offset $\psi \neq 0$, then (6.13) can be expressed as $\alpha_n = \alpha'[\Phi(n\tau + \tau/2 - \psi) - \Phi(n\tau - \tau/2 - \psi)]$ when $d = 0$. Thus, when $\psi = \tau/2$, $\alpha_n = \alpha'[\Phi(n\tau) - \Phi(n\tau - \tau)]$ which is calculated explicitly by

$$\alpha_n = \int_{n\tau-\tau}^{n\tau} p_{\mathcal{N}'}(x) dx. \tag{E.21}$$

Next note that

$$\lim_{\tau\to\infty}\int_{n\tau-\tau}^{n\tau} p_{\mathcal{N}'}(x)dx\Big|_{\forall n<0} = \int_{-\infty}^{-\infty} p_{\mathcal{N}'}(x)dx = 0. \tag{E.22}$$

It then follows from the fact that $p_{\mathcal{N}'}(x)$ is even that

$$\lim_{\tau\to\infty}\int_{n\tau-\tau}^{n\tau} p_{\mathcal{N}'}(x)dx\Big|_{\forall n>1} = \int_{\infty}^{\infty} p_{\mathcal{N}'}(x)dx = 0. \tag{E.23}$$

Conversely, when $n \in \{0, 1\}$

$$\lim_{\tau\to\infty}\int_{n\tau-\tau}^{n\tau} p_{\mathcal{N}'}(x)dx\Big|_{n=0} = \int_{-\infty}^{0} p_{\mathcal{N}'}(x)dx = \frac{1}{2} \tag{E.24}$$

and

$$\lim_{\tau\to\infty}\int_{n\tau-\tau}^{n\tau} p_{\mathcal{N}'}(x)dx\Big|_{n=1} = \int_{0}^{\infty} p_{\mathcal{N}'}(x)dx = \frac{1}{2}. \tag{E.25}$$

□

Next, continuing with the proof of Theorem A5, the resulting Fourier transform of (E.20) is

$$\begin{aligned} P_{\mathcal{N}'}(\phi) &= \int_{-\infty}^{\infty}\left(\frac{1}{2}\delta(x+\tau/2) + \frac{1}{2}\delta(x-\tau/2)\right)e^{-j\phi x}dx \\ &= \frac{1}{2}e^{-j\phi\tau/2} + \frac{1}{2}e^{j\phi\tau/2} \\ &= \cos(\phi\tau/2). \end{aligned} \tag{E.26}$$

Next substituting (E.26) into (E.3) we have

$$\begin{aligned} -\frac{d^2 P_{\mathcal{N}'}(\phi)}{d\phi^2}\Big|_{\phi=0} &= -\frac{d^2}{d\phi^2}\cos(\phi\tau/2)\Big|_{\phi=0} \\ &= -\frac{d}{d\phi}\frac{\tau}{2}\sin(\phi\tau/2)\Big|_{\phi=0} \\ &= \frac{\tau^2}{4}\cos(\phi\tau/2)\Big|_{\phi=0} \\ &= \frac{\tau^2}{4}. \end{aligned} \tag{E.27}$$

Finally, letting $\tau \to \infty$ we have

$$\lim_{\tau\to\infty} - \left.\frac{d^2 P_{\mathcal{N}'}(\phi)}{d\phi^2}\right|_{\phi=0} = \lim_{\tau\to\infty} \frac{\tau^2}{4} = \infty. \quad \blacksquare \tag{E.28}$$

APPENDIX F:
Proof that $P_{\mathcal{N}'}(0) = A_0(0)$, $\forall\psi$ when $\tau = \epsilon$

Theorem A6: *If $p_{\mathcal{N}}(x)$ is normally distributed with variance σ^2 then when $\tau = \epsilon$*

$$P_{\mathcal{N}'}(\phi) = A_0(\phi) \tag{F.1}$$

for sufficiently small ϵ.

Proof: Let $\psi = 0$ and consider the definition

$$P_{\mathcal{N}'}(\phi) = \sum_n A_n(\phi - 2\pi n/\tau) \tag{F.2}$$

where it was previously shown in Chapter 6 that

$$A(\phi) = e^{\frac{-(\phi\sigma)^2}{2}} \operatorname{sinc}\left(\frac{\phi\tau}{2}\right) \tag{F.3}$$

under the assumption that $p_{\mathcal{N}}(x)$ is normally distributed with variance σ^2 and $p_U(x)$ is uniformly distributed $\in [-\tau/2, \tau/2]$. Each copy of (F.3) represented in the sum (F.2) as shifted from the origin by $2\pi n/\tau$ (observe also that (F.3) is even).

It is clear that

$$\lim_{\tau\to 0} \frac{2\pi n}{\tau} = \infty. \tag{F.4}$$

Therefore, all terms in (F.2) where $n \neq 0$ will be centered at $\pm\infty$. Now when $\tau = \epsilon$ the summand when $n = 1$ is centered at $2\pi/\epsilon$ which $\approx \infty$ for sufficiently small ϵ.

Lemma A7:

$$\lim_{\phi\to\pm\infty} A(\phi) = 0. \tag{F.5}$$

Proof: Consider the Gaussian multiplicand in (F.3) which is piece-wise monotonic about its mean and independent of τ. Note that at its extrema

$$\lim_{\phi\to-\infty} e^{\frac{-(\phi\sigma)^2}{2}} = \lim_{\phi\to\infty} e^{\frac{-(\phi\sigma)^2}{2}} = 0. \tag{F.6}$$

Therefore, from the property that

$$\lim_{x\to z} f \cdot h = \left(\lim_{x\to z} f\right) \cdot \left(\lim_{x\to z} h\right) \tag{F.7}$$

the lemma follows. □

Now for the shifted versions of (F.3) we have that

$$\lim_{\phi\to 0} e^{\frac{-((\phi-2\pi n/\epsilon)\sigma)^2}{2}} \operatorname{sinc}\left(\frac{(\phi-2\pi n/\epsilon)\epsilon}{2}\right)\bigg|_{n\neq 0} = \lim_{\phi\to\infty} e^{\frac{-(\phi\sigma)^2}{2}} \operatorname{sinc}\left(\frac{\phi\epsilon}{2}\right)\bigg|_{n\neq 0} = 0 \tag{F.8}$$

where the equality to zero follows from Lemma A7. Therefore, $A_n(0) \approx 0$, $\forall A_n$ where $n \neq 0$ and the contributions in the sum of (F.2) by A_n where $n \neq 0$ are effectively null. In other words

$$\sum_n A_n(\phi - 2\pi n/\epsilon)\bigg|_{\phi=0} = \cdots 0 + 0 + A_0(0) + 0 + 0 + \cdots \tag{F.9}$$

and it can thus be concluded that

$$P_{\mathcal{N}'}(\phi)|_{\phi=0,\tau=\epsilon} = \sum_n A_n(0 - 2\pi n/\epsilon) = A_0(0) \tag{F.10}$$

when $\psi = 0$. Now let $\psi \neq 0$ then (F.2) becomes

$$P_{\mathcal{N}'}(\phi)|_{\psi\neq 0} = e^{-j\phi\psi} \sum_n A_n(\phi - 2\pi n/\tau) \tag{F.11}$$

and

$$A(\phi) = e^{-j\phi\psi} e^{\frac{-(\phi\sigma)^2}{2}} \operatorname{sinc}\left(\frac{\phi\tau}{2}\right). \tag{F.12}$$

Here, (F.9) still applies and so Lemma A7 is still valid for $\psi \neq 0$. Now

$$P_{\mathcal{N}'}(\phi)|_{\phi=0,\tau=\epsilon,\psi\neq 0} = e^{-j0\psi} \sum_n A_n(0 - 2\pi n/\epsilon) = A_0(0) \tag{F.13}$$

so that the theorem holds $\forall\psi$. ■

APPENDIX G:
Sufficient Condition for $\mathrm{Var}(\mathcal{N}') \geq \mathrm{Var}(\mathcal{N})$

Theorem A7: *The lower bound on the RMSE for a RV after quantization will always be higher than the CRLB iff*

$$\tau \lesssim 3.4\sigma. \tag{G.1}$$

Proof: It has been previously shown in Appendix E that the minimum value of $\mathrm{Var}(\mathcal{N}')$ occurs when there is no annular offset (i.e., $\text{Ш}_\tau(x-0)$). Therefore, since this value of ψ results in minimum variance in the quantized RV $\mathcal{N}'$ and the variance of $\mathcal{N}'$ for all other offsets such that $\psi \neq 0$ will be equal to or larger than $\mathcal{N}$, this is the only condition which needs evaluation. The variance of $\mathcal{N}'$ for $\psi = 0$ is given by

$$\begin{aligned}
\mathrm{Var}(\mathcal{N}') &= \int_{-\infty}^{\infty} x^2 \alpha_n \delta(x - n\tau) dx \\
&= \sum_{n=-\infty}^{\infty} (n\tau)^2 a_n \\
&= \sum_{n=-\infty}^{\infty} (n\tau)^2 \int_{n\tau-\tau/2}^{n\tau+\tau/2} p_{\mathcal{N}}(x) dx
\end{aligned} \tag{G.2}$$

where $\Phi(x)$ is the cumulative density of x. The first step follows from the definition of variance of a zero mean random variable. The second step follows from $f(x)\delta(x-a) = f(a)\delta(x-a)$ and $\int \delta(x)dx = 1$. The third step follows from $a_n = \int_{q_n} p_{\mathcal{N}}(x)dx$ where the definite integral is over the interval q_n. To see this recall that

$$\begin{aligned}
p_{\mathcal{N}'}(x) &= \text{Ш}_\tau(x) \left(p_{\mathcal{N}}(x) * p_U(x)\right) \\
&= \sum_{n=-\infty}^{\infty} \delta(x - n\tau) \left(p_{\mathcal{N}}(x) * p_U(x)\right) \\
&= \sum_{n=-\infty}^{\infty} \delta(x - n\tau) \left(\Phi(x + \tau/2) - \Phi(x - \tau/2)\right) \\
&= \sum_{n=-\infty}^{\infty} \delta(x - n\tau) \left(\Phi(n\tau + \tau/2) - \Phi(n\tau - \tau/2)\right)
\end{aligned} \tag{G.3}$$

$$= \sum_{n=-\infty}^{\infty} \delta(x - n\tau) \int_{n\tau-\tau/2}^{n\tau+\tau/2} p_{\mathcal{N}}(x)dx. \tag{G.4}$$

Therefore,

$$a_n = \int_{n\tau-\tau/2}^{n\tau+\tau/2} p_{\mathcal{N}}(x)dx. \tag{G.5}$$

Now, as a first approximation of $p_{\mathcal{N}'}(x)$, assume that $\tau > \epsilon$ so that

$$p_{\mathcal{N}'}(x)_1 = a_{-1}\delta(x + \tau) + a_0\delta(x) + a_1\delta(x - \tau) \tag{G.6}$$

where the subscript 1 denotes the indices of a_n considered in the approximation. Applying (G.2) to (G.6) we have

$$\begin{aligned} \mathrm{Var}(\mathcal{N}')_1 &= (-\tau)^2\Phi\left(\frac{-\tau}{2}\right) + (0)^2\left(\Phi\left(\frac{\tau}{2}\right) - \Phi\left(\frac{-\tau}{2}\right)\right) + (\tau)^2\left(1 - \Phi\left(\frac{\tau}{2}\right)\right) \\ &= (-\tau)^2\Phi\left(\frac{-\tau}{2}\right) + (\tau)^2\Phi\left(\frac{-\tau}{2}\right) \\ &= 2\tau^2\Phi\left(\frac{-\tau}{2}\right) \end{aligned} \tag{G.7}$$

which leads to

$$2\tau^2\Phi\left(\frac{-\tau}{2}\right) \lesssim \sigma^2. \tag{G.8}$$

Then solving for τ we have

$$\tau \lesssim 3.4\sigma. \tag{G.9}$$

To begin to quantify the fidelity of the approximation given in (G.6) let it be extended to

$$p_{\mathcal{N}'}(x)_2 = a_{-2}\delta(x + 2\tau) + a_{-1}\delta(x + \tau) + a_0\delta(x) + a_1\delta(x - \tau) + a_2\delta(x - 2\tau). \tag{G.10}$$

In this case the variance is given by

$$\begin{aligned} \mathrm{Var}(\mathcal{N}')_2 &= (-2\tau)^2\Phi\left(\frac{-3\tau}{2}\right)(-\tau)^2\left(\Phi\left(\frac{-\tau}{2}\right) - \Phi\left(\frac{-3\tau}{2}\right)\right) \\ &\quad + (\tau)^2\left(\Phi\left(\frac{3\tau}{2}\right) - \Phi\left(\frac{\tau}{2}\right)\right) + (2\tau)^2\left(1 - \Phi\left(\frac{3\tau}{2}\right)\right) \\ &= 8\tau^2\Phi\left(\frac{-3\tau}{2}\right) + 2\tau^2\left(\Phi\left(\frac{-\tau}{2}\right) - \Phi\left(\frac{-3\tau}{2}\right)\right). \end{aligned} \tag{G.11}$$

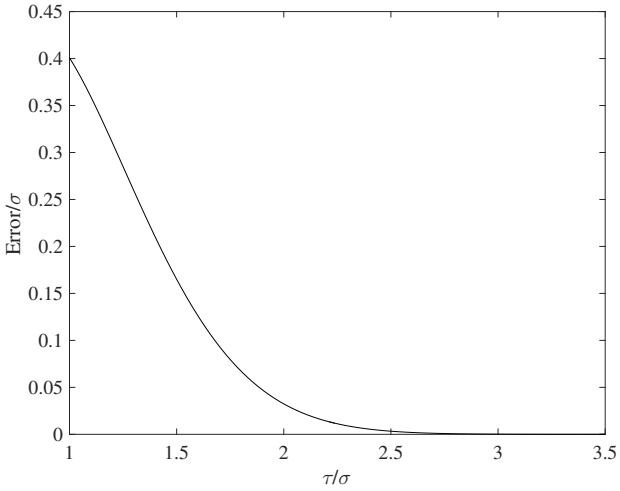


Figure G.1. The error associated with using the first-order variance approximation parameterized by τ is presented in this figure. Both the resulting error and τ are normalized by σ.

Now in order to understand when the first order approximation given in (G.6) is no longer valid, consider the difference between the two approximations of variance

$$\mathrm{Var}(\mathcal{N}')_2 - \mathrm{Var}(\mathcal{N}')_1 = 6\tau^2\Phi\left(\frac{-3\tau}{2}\right). \tag{G.12}$$

The resulting error between the two approximations of $\mathrm{Var}(\mathcal{N}')$ is shown in Figure G.1. By inspection, one finds that the initial first-order approximation is appropriate for finding the upper bound on τ since the error associated with $p_{\mathcal{N}'}(x)_1$ is negligible. Specifically, the error associated with using the first-order approximation at $\tau = 3.4$ is 1.1779×10^{-5}. One may thus conclude that further approximation of the bound is not necessary and that the sufficient condition for $\mathrm{Var}(\mathcal{N}') \geq \mathrm{Var}(\mathcal{N})$ is $\tau \lesssim 3.4\sigma \; \forall\psi$. ■

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX H:
Link Budget for Empirical CeSAR Validation

When conducting the empirical CeSAR validation accurate distance estimates were highly dependent on the strength of the received signal. This appendix details the solution approach taken to ensure the received signal was strong enough to provide a distance estimate.

Among the challenges associated with the hardware was inter-chain leakage, transmit power limitations, and large losses associated with free space transmission and cable propagation. The transmit and receive chains had an approximate isolation of 40 dB, therefore, if the received signal was not strong enough the leakage signal would dominate and the measurement would be corrupted. The resulting distance estimate would be zero meters since there is a negligible propagation delay for the leakage signal.

Additionally, the USRP transmit and receive gain variables are not well defined and do not necessarily translate to dBm[48]. Our measurements indicated the USRP gain values corresponded to the transmit powers via the relationships shown in Table H.1. The transmit power was measured with a spectrum analyzer as the peak power at the transmit frequency for a BPSK sequence.

Table H.1. Correlation between USRP gain values and actual transmit powers

USRP Gain Value	Transmit Power (dBm)
0	-10
20	9.65
26	15.41
30	18.32
40	18.64

In order to determine the link budget associated with the experiment in Chapter 8, we now enumerate the losses associated with the system used which is shown in Figure H.1. First, the loss associated with the coaxial cable was given by the manufacturer as -12.6 dB/100 m. For the 150 m length of cable used in this experiment the total loss is theoretically 18.9 dB

[48]In other words, a transmit gain of 20 $\neq$ 20 dBm.

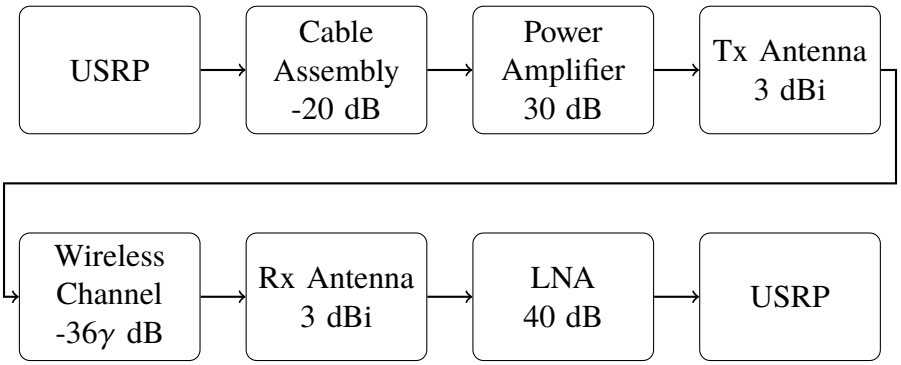


Figure H.1. The link budget of the CeSAR validation experiment

and was measured at ≈ 20 dB.

The loss associated with wireless transmission L can be calculated as

$$L = 10\gamma \log\left(\frac{4\pi d}{\lambda}\right) \tag{H.1}$$

where γ is the path loss exponent, d is the distance of the wireless channel, and λ is the wavelength. When transmitting at 915.1 MHz for a 100 m wireless channel this results in a path loss of ≈72 dB to ≈143 dB assuming a path loss exponent of 2 and 4 respectively.

The overall system loss was overcome with a medium power amplifier on the transmit antenna and a low noise amplifier on the receive antenna. The signal is first attenuated by the cable assembly, then amplified by the medium power amplifier before it is broadcast at the transmit antenna. Assuming the USRP transmits at 15 dBm (cf. Table H.1) this means the transmit power before the Tx antenna is 25 dBm. Standard dipole antennas (3 dBi) were used for transmission and reception. The signal then experiences path loss from the wireless channel before it is amplified by the 40 dB low noise amplifier. The overall system loss including amplifier gains is -16 dB to -87 dB for a γ of 2 to 4 respectively.

The length of the PN sequence was also leveraged to increase the processing gain. In our case, a 12th order LFSR was used which corresponds to 4095 bits or ≈ 36 dB of processing gain.

Assuming the USRP does transmit at 15 dBm then the received signal power, before it is amplified by internal USRP amplifiers is anywhere from -1 dBm to -72 dBm. Finally, after

amplification from internal power amplifiers, the resulting correlation peak is then amplified in processing by 36 dB. Due to the potential for received signals to have very low power, the magnitude of the correlation peak is used to validate the reception of a sufficiently strong signal. If the correlation peak is significantly larger than the correlation noise floor a valid distance measurement is recorded.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX I:
GNU Radio Code for Generating a BPSK PN Sequence and Synchronizing USRP Tx/Rx Chains

```
#!/usr/bin/env python2
# -*- coding: utf-8 -*-
##################################################
# GNU Radio Python Flow Graph
##################################################

from gnuradio import blocks
from gnuradio import digital
from gnuradio import eng_notation
from gnuradio import gr
from gnuradio import uhd
from gnuradio.eng_option import eng_option
from gnuradio.filter import firdes
from optparse import OptionParser
import time
import numpy as np
import matplotlib.pyplot as plt
import os


class gnuradioflow(gr.top_block):

    def __init__(self):
        gr.top_block.__init__(self, "Gnuradioflow")

        ##################################################
        # Variables
        ##################################################
        self.samp_rate = samp_rate = 25e6
```

```
        self.constellation = constellation =
            digital.constellation_calcdist(([-1, 1]), ([0, 1]), 4, 1).base()
        self.center_freq = center_freq = 915.1e6

        ##################################################
        # Blocks
        ##################################################
        self.usrp_source = uhd.usrp_source(
         ",".join(("", "")),
         uhd.stream_args(
            cpu_format="fc32",
            channels=range(1),
         ),
        )
        self.usrp_source.set_samp_rate(samp_rate)
        self.usrp_source.set_center_freq(center_freq, 0)
        self.usrp_source.set_gain(20, 0) #Receive chain amplifier gain
        self.usrp_source.set_antenna("RX2", 0)
        self.usrp_source.set_bandwidth(samp_rate, 0)
        self.usrp_sink = uhd.usrp_sink(
         ",".join(("", "")),
         uhd.stream_args(
            cpu_format="fc32",
            channels=range(1),
         ),
        )
        self.usrp_sink.set_samp_rate(samp_rate)
        self.usrp_sink.set_center_freq(center_freq, 0)
        self.usrp_sink.set_gain(26, 0) #Transmit chain amplifier gain
        self.usrp_sink.set_antenna("TX/RX", 0)
        self.usrp_sink.set_bandwidth(samp_rate, 0)

    ##################################################
    # Approximate measured gains for URSP gain value
    #  - Measured as peak value of BPSK signal
```

```
##################################################
# USRP Gain Value Actual Gain
#
# 0        -10dBm
# 20       9.65 dBm
# 26       15.41 dBm
# 30       18.32 dBm
# 40       18.64 dBm
##################################################

##################################################################
# Synchronize Tx/Rx Chains (starts chains 100ms in the future)
##################################################################
start_time=self.usrp_sink.get_time_now().get_real_secs()+.1
self.usrp_sink.set_start_time(uhd.time_spec(start_time))
self.usrp_source.set_start_time(uhd.time_spec(start_time))

    self.digital_glfsr_source_x_0 = digital.glfsr_source_b(12, False,
       0, 1) #sets GLFSR order to 12
    self.digital_constellation_modulator_0 = digital.generic_mod(
      constellation=constellation,
      differential=True,
      samples_per_symbol=2,
      pre_diff_code=True,
      excess_bw=0.35,
      verbose=False,
      log=False,
      )
    self.blocks_multiply_const_vxx_0 = blocks.multiply_const_vcc((0.5,
       )) #prevents overloading amplifiers during Tx
    self.blocks_head_0 = blocks.head(gr.sizeof_gr_complex*1,
       int(samp_rate/1000)) #sets number of samples of the rxwave to
       save
    self.blocks_file_sink_1 = blocks.file_sink(gr.sizeof_gr_complex*1,
       "/home/USER/Desktop/rxwave", False) #location to save rxwave
```

```
        self.blocks_file_sink_1.set_unbuffered(False)
        self.blocks_file_sink_0 = blocks.file_sink(gr.sizeof_gr_complex*1,
            "/home/USER/Desktop/txwave", False) #location to save txwave
        self.blocks_file_sink_0.set_unbuffered(False)

        ##################################################
        # Connections
        ##################################################
        self.connect((self.blocks_head_0, 0), (self.blocks_file_sink_1, 0))
        self.connect((self.blocks_multiply_const_vxx_0, 0),
            (self.usrp_sink, 0))
        self.connect((self.digital_constellation_modulator_0, 0),
            (self.blocks_file_sink_0, 0))
        self.connect((self.digital_constellation_modulator_0, 0),
            (self.blocks_multiply_const_vxx_0, 0))
        self.connect((self.digital_glfsr_source_x_0, 0),
            (self.digital_constellation_modulator_0, 0))
        self.connect((self.usrp_source, 0), (self.blocks_head_0, 0))

    def get_samp_rate(self):
        return self.samp_rate

    def set_samp_rate(self, samp_rate):
        self.samp_rate = samp_rate
        self.blocks_head_0.set_length(int(self.samp_rate/8))
        self.usrp_sink.set_samp_rate(self.samp_rate)
        self.usrp_sink.set_bandwidth(self.samp_rate, 0)
        self.usrp_source.set_samp_rate(self.samp_rate)
        self.usrp_source.set_bandwidth(self.samp_rate, 0)

    def get_constellation(self):
        return self.constellation

    def set_constellation(self, constellation):
        self.constellation = constellation
```

```
    def get_center_freq(self):
        return self.center_freq

    def set_center_freq(self, center_freq):
        self.center_freq = center_freq
        self.usrp_sink.set_center_freq(self.center_freq, 0)
        self.usrp_source.set_center_freq(self.center_freq, 0)


def main(top_block_cls=gnuradioflow, options=None):

    tb = top_block_cls()
    tb.start()
    tb.wait()

    itr = 10 # Number of automated measurements to take, keep this number
        low in order to avoid burning out the Tx/Rx chains
    samples = range(itr) # The measured distances will be saved here
    corr = range(itr) # This will save the peak correlation value to review
        in post-processing
    thresh = 1500 # This is the threshold the correlation peak must exceed
        in order to be a valid measurement

    for x in range(1, itr+1):
    i = 0
    z = [0]
    while (z[i] < thresh or dist < 0):
        tb = top_block_cls()
        tb.start()
        tb.wait()

        rx_read_complex_binary = np.fromfile('../../Desktop/rxwave',
            dtype=np.complex64)
```

```
        tx_read_complex_binary = np.fromfile('../../Desktop/txwave',
            dtype=np.complex64)
        rx = rx_read_complex_binary.real
        tx = tx_read_complex_binary.real

        z = np.correlate(rx, tx, "full")
        i = np.argmax(abs(z))
        dist = (i - zerodist) * 299792458/tb.samp_rate #Calculate the
            distance from the max correlation index

    print "trial " + str(x) + ": " + str(dist) + " meters, correlation @: "
        + str(i)
    samples[x-1] = dist
    corr[x-1] = abs(z[i])

    #Optionally plot the correlation peak and the received signal
    plt.plot(abs(z))
    plt.show()
    plt.plot(rx)
    plt.show()

    print "mean: " +str(np.mean(samples))
    sl = open('/home/jroth/Desktop/Samples', 'wb+')
    sl.write(str(samples))
    sl.close()
    sl = open('/home/jroth/Desktop/Correlation', 'wb+')
    sl.write(str(corr))
    sl.close()


if __name__ == '__main__':
    main()
```

List of References

[1] Nokia Siemens Networks, "2020: Beyond 4G," *White Paper*, 2011.

[2] Ericsson, "Ericsson mobility report," *White Paper*, 2016.

[3] A. Bleicher, "4G gets real," *IEEE Spectrum*, vol. 51, pp. 38–62, 2014.

[4] "Revision of the commission's rules to ensure compatibility with enhanced 911 emergency calling systems, third report and order," *9 FCC Rcd 17388*, 1999.

[5] J. Bull, "Wireless geolocation," *IEEE Veh. Tech. Mag.*, vol. 4, pp. 45–53, 2009.

[6] A. H. Sayed, A. Tarighat, and N. Khajehnouri, "Network-based wireless location: challenges faced in developing techniques for accurate wireless location information," *IEEE Signal Processing Mag.*, vol. 22, no. 4, pp. 24–40, 2005.

[7] F. Gustafsson and F. Gunnarsson, "Mobile positioning using wireless networks: possibilities and fundamental limitations based on available wireless network measurements," *IEEE Signal Processing Mag.*, vol. 22, no. 4, pp. 41–53, 2005.

[8] A. Roxin, J. Gaber, M. Wack, and A. Nait-Sidi-Moh, "Survey of wireless geolocation techniques," in *Proc. IEEE Globecom Workshops*, 2007, pp. 1–9.

[9] G. Sun, J. Chen, W. Guo, and K. R. Liu, "Signal processing techniques in network-aided positioning: a survey of state-of-the-art positioning designs," *IEEE Signal Processing Mag.*, vol. 22, no. 4, pp. 12–23, 2005.

[10] I. Güvenç and C.-C. Chong, "A survey on TOA based wireless localization and NLOS mitigation techniques," *IEEE Commun. Surveys & Tutorials*, vol. 11, no. 3, pp. 107–124, 2009.

[11] A. Westin, *Privacy and Freedom*, 1st ed. New York: Atheneum, 1967.

[12] A. R. Beresford and F. Stajano, "Location privacy in pervasive computing," *IEEE Pervasive Comput.*, vol. 2, pp. 46–55, 2003.

[13] S. Gambs, M.-C. Killijian, and M. del Prado-Cortez, "De-anonymization attack on geolocated data," in *Proc. IEEE Intl. Conf. Trust, Security, Privacy Comput. Commun.*, 2013, pp. 789–797.

[14] J. Krumm, "A survey of computational location privacy," *Pers. Ubiquit. Comput.*, vol. 13, pp. 391–399, 2009.

[15] L. Barkuus and A. Dey, "Location-based services for mobile telephony: a study of users' privacy concerns," in *Proc. 9th Intl. Conf. Human-Computer Interaction*, 2003, pp. 709–712.

[16] G. Iachello *et al.*, "Control, deception, and communication: evaluating the deployment of a location-enhanced messaging service," in *Proc. ACM Intl. Conf. Pervasive Ubiquitous Comput.*, 2005, pp. 213–231.

[17] E. Kaasinen, "User needs for location-aware mobile services," *Pers. Ubiquit. Comput.*, vol. 7, pp. 70–79, 2003.

[18] M. Bshara, U. Orguner, F. Gustafsson, and L. Van Biesen, "Robust tracking in cellular networks using HMM filters and cell-ID measurements," *IEEE Trans. Veh. Technol.*, vol. 60, no. 3, pp. 1016–1024, 2011.

[19] M. Bshara, U. Orguner, F. Gustafsson, and L. Van Biesen, "Fingerprinting localization in wireless networks based on received-signal-strength measurements: a case study on WiMAX networks," *IEEE Trans. Veh. Tech.*, vol. 59, no. 1, pp. 283–294, 2010.

[20] M. Duckham and L. Kulik, "Location privacy and location-aware computing," in *Dynamic & Mobile GIS: Investigating Change in Space and Time*, J. Drummond, R. Billen, E. Joao, and D. Forrest, Eds. CRC Press, 2006, ch. 3.

[21] J. D. Roth, M. Tummala, J. C. McEachen, J. W. Scrofani, and R. A. DeGabriele, "Maximum likelihood geolocation in LTE cellular networks using the timing advance parameter," in *Proc. 10th Intl. Conf. Signal Process. Commun. Syst.*, to be published, 2016.

[22] E. Dahlman, S. Parkvall, and J. Sköld, *4G LTE/LTE-Advanced for Mobile Broadband*. Academic Press, 2011.

[23] L. Jarvis, J. McEachen, and H. Loomis, "Geolocation of LTE subscriber stations based on the timing advance ranging parameter," in *Proc. Military Commun.*, 2011.

[24] J. D. Roth, M. Tummala, and J. W. Scrofani, "Cellular synchronization assisted refinement (CeSAR): A method for accurate geolocation in LTE-A networks," in *Proc. 49th Hawaii Int. Conf. Syst. Sci.*, 2016, pp. 5842–5850.

[25] G. Yost and S. Panchapakesan, "Improvement in estimation of time of arrival (TOA) from timing advance (TA)," in *Proc. IEEE Intl. Conf. Universal Personal Commun.*, 1998, pp. 1367–1372.

[26] M. Raitoharju, S. Ali-Löytty, and L. Wirola, "Estimation of base station position using timing advance measurements," in *Proc. Intl. Conf. Graphic Image Process.*, 2011.

[27] C. Fritsche and A. Klein, "On the performance of mobile terminal tracking in urban GSM networks using particle filters," 2009, pp. 1953–1957.

[28] J. D. Roth, M. Tummala, J. C. McEachen, and J. W. Scrofani, "Location privacy in LTE: A case study on exploiting the cellular signaling plane's timing advance," in *Proc. 50th Hawaii Int. Conf. Syst. Sci.*, to be published, 2017.

[29] J. D. Roth, M. Tummala, J. C. McEachen, and J. W. Scrofani, "On location privacy in LTE networks," submitted for publication.

[30] U. Hammes, E. Wolsztynski, and A. Zoubir, "Robust tracking in geolocation for wireless networks in NLOS environments," *IEEE J. Sel. Topics Sig. Process.*, vol. 3, no. 5, pp. 889–901, 2009.

[31] Y.-T. Chan, W.-Y. Tsui, H.-C. So, and P.-C. Ching, "Time-of-arrival based localization under NLOS conditions," *IEEE Trans. Veh. Tech.*, vol. 55, no. 1, pp. 17–24, 2006.

[32] M. Kayton and W. Fried, *Avionics Navigation Systems*. Wiley, 1997.

[33] M. H. Kabir and R. Kohno, "A geolocation approach using UWB deterministic modeling for non line-of-sight conditions," in *Proc. IEEE 6th Int. Symp. Medical Inform. Commun. Tech.*, 2012, pp. 1–4.

[34] W. Q. Malik and B. Allen, "Wireless sensor positioning with ultrawideband fingerprinting," in *IEEE 1st European Conf. Antennas Propagation*, 2006, pp. 1–5.

[35] C. Feng, W. S. A. Au, S. Valaee, and Z. Tan, "Compressive sensing based positioning using RSS of WLAN access points," in *Proc. IEEE Int. Conf. Comput. Commun.*, 2010, pp. 1–9.

[36] R. Xu and T. Jiang, "Keeping track of position and cell residual dwell time of cellular networks using HSMM structure and cell-ID information," in *Proc. IEEE Int. Conf. Commun.*, 2012, pp. 6411–6415.

[37] J. Henderson, M. Tummala, J. McEachen, and J. Scrofani, "Scheme for enhanced tracking of mobile subscribers in a WiMAX network," in *Proc. IEEE 6th Int. Conf. Signal Process. Commun. Syst.*, 2012, pp. 1–4.

[38] T. Wigren, "Fingerprinting localisation using round trip time and timing advance," *IET Commun.*, vol. 6, pp. 419–427, 2012.

[39] 3GPP TS 36.355, release 10, (v10.12.0), "Evolved Universal Terrestrial Radio Access (E-UTRA); LTE Positioning Protocol (LPP)," July 2014.

[40] C. Drane, M. Macnaughtan, and C. Scott, "Positioning GSM telephones," *IEEE Commun. Mag.*, vol. 36, no. 4, pp. 46–54, 1998.

[41] J. Jin, Z.-J. Qui, and B. Ran, "Intelligent route-based speed estimation using timing advance," in *Proc. IEEE Intell. Transportation Syst. Conf.*, 2006, pp. 194–197.

[42] R. Whitty, M. Tummala, and J. McEachen, "Precision geolocation of mobile WiMAX subscribers using timing adjust measurements," in *Proc. 45th Hawaii Int. Conf. Sys. Sci.*, 2012, pp. 5639–5648.

[43] T.-H. Ngo and Y. Kim, "Using timing advance to support proximity discovery in network-assisted D2D communication," in *Proc. Intl. Conf. Ubiquit. Future Net.*, 2015, pp. 926–928.

[44] T. Hiltunen, J. Turkka, R. Mondal, and T. Ristaniemi, "Performance evaluation of LTE radio fingerprint positioning with timing advancing," in *Proc. Intl. Conf. Info. Commun. Sig. Process.*, 2015.

[45] Ericsson, "Positioning with LTE," *White Paper*, 2011.

[46] 3GPP TR 36.809, (v1.0.0), "Radio Frequency (RF) pattern matching method in LTE," Aug. 2013.

[47] 3GPP TS 33.401, release 9, (v9.7.0), "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3GPP System Architecture Evolution (SAE); Security Architecture (Release 9)," June 2011.

[48] M. DeGroot and M. Schervish, *Probability and Statistics*, 4th ed. Pearson, 2012.

[49] C. W. Therrien and M. Tummala, *Probability for electrical & computer engineers*. CRC Press, 2004.

[50] 3GPP TS 36.321, release 10, (v10.10.0), "Evolved Universal Terrestrial Radio Access (E-UTRA); Medium Access Control (MAC) protocol specification," Dec. 2012.

[51] 3GPP TS 36.211, release 10, (v10.7.0), "Evolved Universal Terrestrial Radio Access (E-UTRA); Physical Channels and Modulation," Feb. 2013.

[52] 3GPP TS 36.213, release 10, (v10.12.0), "Evolved Universal Terrestrial Radio Access (E-UTRA); Physical Layer Procedures," Mar. 2014.

[53] 3GPP TS 36.214, release 9, (v9.2.0), "Evolved Universal Terrestrial Radio Access (E-UTRA); Physical Layer; Measurements," June 2010.

[54] 3GPP TS 36.331, release 10, (v10.16.0), "Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Resource Control (RRC); Protocol specification," Mar. 2015.

[55] P. Bhat, S. Nagata, L. Campoy, I. Berberana, T. Derham, G. Liu, X. Shen, P. Zong, and J. Yang, "LTE-advanced: an operator perspective," *IEEE Commun. Mag.*, vol. 50, no. 2, pp. 104–114, 2012.

[56] M. Zhou and L. Wan, "Analysis into timing advance issue in CoMP systems," in *Proc. 70th IEEE Veh. Tech. Conf.*, 2009, pp. 1–5.

[57] Y. Moon, S. Bahng, J. Kim, Y. Park, and W. Kim, "RRH selection and ue transmission timing adjustment for LTE-Advanced uplink MU-MIMO in distributed antenna system environment," in *Proc. Int. Conf. Inform. Commun. Tech. Convergence*, 2014, pp. 301–305.

[58] R. Shokri, G. Theodorakopoulos, J.-Y. Le Boudec, and J.-P. Hubaux, "Quantifying location privacy," in *Proc. IEEE Symp. Security Privacy*, 2011, pp. 247–262.

[59] J. Cao, M. Ma, H. Li, Y. Zhang, and Z. Luo, "A survey on security aspects for LTE and LTE-A networks," *IEEE Commun. Surveys Tutorials*, vol. 16, no. 1, pp. 283–302, 2014.

[60] I. Bilogrevic, M. Jadliwala, and J.-P. Hubaux, "Security and privacy in next generation mobile networks: LTE and femtocells," *Femotcell Workshop*, 2010.

[61] J. D. Roth, M. Tummala, J. McEachen, and J. Scrofani, "On mobile positioning via cellular synchronization assisted refinement (CeSAR) in LTE and GSM networks," in *Proc. 9th Int. Conf. Signal Process. Commun. Syst.*, 2015.

[62] J. Eberspächer, J. Betterstetter, and H.-J. Vögel, *GSM - architecture, protocols, and services*, 3rd ed. Wiley, 2009.

[63] 3GPP TS 45.002, release 10, (v10.5.0), "3rd Generation Partnership Project; Technical Specification Group GSM/EDGE Radio Access Network; Multiplexing and multiple access on the radio path," Aug. 2013.

[64] 3GPP TS 43.020, release 9, (v9.2.0), "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Security related network functions," June 2014.

[65] B. Widrow, I. Kollár, and M.-C. Liu, "Statistical theory of quantization," *IEEE Trans. Instrum. Meas.*, vol. 45, no. 2, pp. 353–361, 1996.

[66] Y. Qi, H. Kobayashi, and H. Suda, "Analysis of wireless geolocation in a non-line-of-sight environment," *IEEE Trans. Wireless Commun.*, vol. 5, no. 3, pp. 672–681, 2006.

[67] L. Greenstein, V. Erceg, Y. Yeh, and M. Clark, "A new path-gain/delay-spread propagation model for digital cellular channels," *IEEE Trans. Veh. Tech.*, vol. 46, no. 2, pp. 477–485, 1997.

[68] H. Dhilion and C. Gomez, "Small cells big gains: Increasing cellular capacity," IEEE Communications Society Webinar, Mar 2015.

[69] W. Sheppard, "On the calculation of the most probable values of frequency-constants, for data arranged according to equidistant divisions of scale," in *Proc. London Math. Soc.*, 1898, pp. 353—-380.

[70] B. Widrow, "A study of rough amplitude quantization by means of Nyquist sampling theory," 1956, Sc.D. Thesis.

[71] B. Widrow, "A study of rough amplitude quantization by means of Nyquist sampling theory," *IRE Trans. Circuit Theory*, vol. 3, no. 4, pp. 266—-276, 1956.

[72] B. Widrow, I. Kollár, and M.-C. Liu, "Statistical analysis of amplitude-quantized sampled-data systems," *Trans. AIEE, Part II: Applicat. Ind.*, vol. 79, no. 52, pp. 555—-568, 1961.

[73] J. Caffery and G. Stuber, "Overview of radiolocation in CDMA cellular systems," *IEEE Commun. Mag.*, vol. 36, no. 4, pp. 38–45, 1998.

[74] J. D. Roth, M. Tummala, J. McEachen, and J. Scrofani, "A configurable fingerprint-based hidden-Markov model for tracking in variable channel conditions," in *Proc. 7th Int. Conf. Signal Process. Commun. Syst.*, 2013.

[75] S. Rao, "Classical statistical inference," lecture notes.

[76] M. Abramowitz and I. Stegun, *Handbook of Mathematical Functions with Formulas, Graphs, and Mathematical Tables, 9th printing*, 3rd ed. New York: Dover Publications, 1972.

Initial Distribution List

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California